FortiAuthenticator v3.0
Administration Guide

FortiAuthenticator v3.0 Administration Guide

November 29, 2013

23-300-144822-20131129

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Table of Figures

Change Log

Date	Change Description
2013-11-29	Initial Release.

Introduction

The FortiAuthenticator device is an authentication server. Authentication servers are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

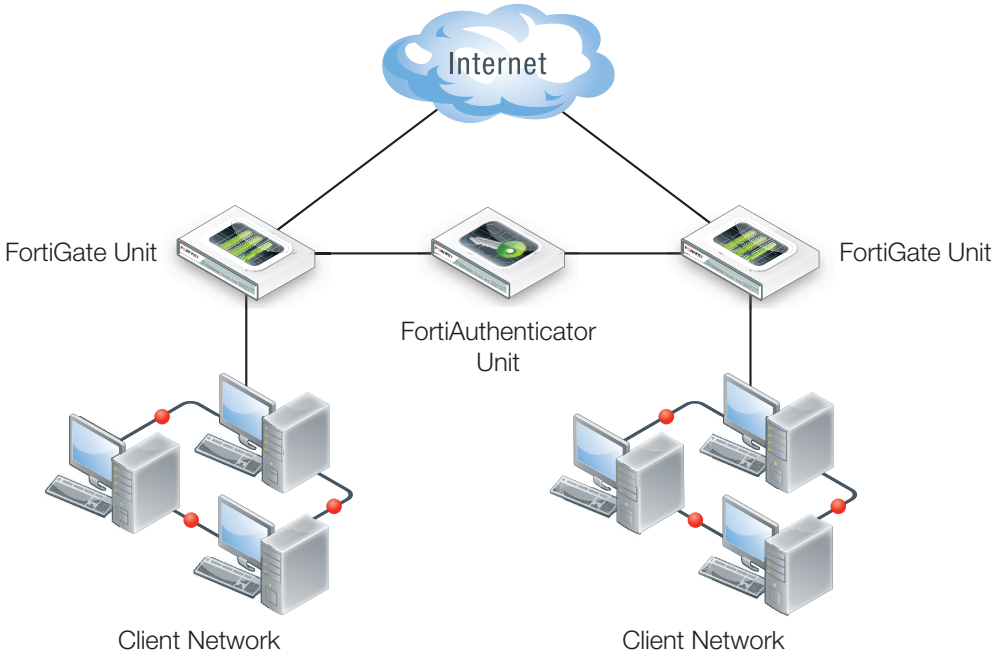
FortiAuthenticator provides user identity services to the Fortinet product range, as well as third party devices.

FortiAuthenticator delivers multiple features including:

- *Authentication*: FortiAuthenticator includes Remote Authentication Dial In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) server authentication methods.
- *Two Factor Authentication*: FortiAuthenticator can act as a two-factor authentication server with support for one-time passwords using FortiToken 200, FortiToken Mobile, SMS, or e-mail. FortiAuthenticator two-factor authentication is compatible with any system which supports RADIUS.
- *IEEE802.1X Support*: FortiAuthenticator supports 802.1X for use in FortiGate Wireless and Wired networks.
- *User Identification*: FortiAuthenticator can identify users through multiple data sources, including Active Directory, Desktop Client, Captive Portal Logon, RADIUS Accounting, and a Representational State Transfer (REST) API. It can then communicate this information to FortiGate, FortiCache, or FortiMail units for use in Identity Based Policies.
- *Certificate Management*: FortiAuthenticator can create and sign digital certificates for use, for example, in FortiGate VPNs and with the FortiToken 300 USB Certificate Store.

FortiAuthenticator is a server and should be isolated on a network interface separate from other hosts to facilitate server-related firewall protection. Be sure to take steps to prevent unauthorized access to the FortiAuthenticator.

Figure 1: FortiAuthenticator on a multiple FortiGate unit network



The FortiAuthenticator series of secure authentication appliances complements the FortiToken range of two-factor authentication tokens for secure remote access. FortiAuthenticator allows you to extend the support for FortiTokens across your enterprise by enabling authentication with multiple FortiGate appliances and third party devices. FortiAuthenticator and FortiToken deliver cost effective, scalable secure authentication to your entire network infrastructure.

The FortiAuthenticator device provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the FSSO Agent on a Windows Active Directory network.

For more information about FortiTokens, see the FortiToken information page on the Fortinet web site.

This chapter contains the following topics:

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.

  For details of how to accomplish this, see the QuickStart Guide provided with your product, or online at http://docs.fortinet.com/fauth.html.
- The FortiAuthenticator unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.

Network Time Protocol (NTP) is critical for the time to be accurate and stable for the Time-based One-time Password (TOTP) method used in two-factor authentication to function correctly. See “Configuring the system time, time zone, and date” on page 36.

- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to have all permissions, unless otherwise specified. Some restrictions will apply to administrators with limited permissions.

How this guide is organized

This FortiAuthenticator Administration Guide contains the following sections:

- Setup describes initial setup for standalone and HA cluster FortiAuthenticator configurations.
- System describes the options available in the system menu tree, including: network configuration, administration settings, and messaging settings.
- Authentication describes how to configure built-in and remote authentication servers and manage users and user groups.
- Port-based Network Access Control describes how to configure the FortiAuthenticator unit for IEEE 802.1X EAP authentication methods, BYOD, and MAC-based device authentication.
- Fortinet Single Sign-On describes how to use the FortiAuthenticator unit in a single sign on (SSO) environment.
- RADIUS Single Sign-On describes how to use the FortiAuthenticator unit RADIUS accounting proxy.
- Monitoring describes how to monitor SSO and authentication information.
- Certificate Management describes how to manage X.509 certificates and how to set up the FortiAuthenticator unit to act as an Certificate Authority (CA).
- Logging describes how to view the logs on your FortiAuthenticator unit.
- Troubleshooting provides suggestions to resolve common problems.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

What's New

FortiAuthenticator v3.0 includes the following new features and enhancements.

Always review all sections in the *FortiAuthenticator Release Notes* prior to upgrading your device.

System features

These features are related to general system operation and not a specific functional area.

Web-based Manager reorganization

To reflect the changes that have been made in this FortiAuthenticator release, the Web-based Manager Graphical User Interface (GUI) has been reorganized and adjusted to improve clarity and usability.

Under the *Authentication* menu:

- *RADIUS Service* tree menu has been added that includes NAS Client and Extensible Authentication Protocol (EAP) configuration options
- *LDAP Service* tree menu has been added that includes general and directory tree settings
- Dedicated tree menu has been created for the self-service portal features
- *Lockouts* has been moved to it's own menu under the *User Account Policies* tree menu.

Under the *System* menu:

- *Maintenance* tree menu has been renamed to *Administration*, and submenus have been added for *GUI Access* and *FortiGuard*
- *FTP Servers* menu has been moved from *Logging* > *Log Config* to *System* > *Administration*.

Multilingual support for user interface

Support has been added for the customization of the language of various elements of the Web-based Manager and SMS and email messages. A set of default supported language files will be provided.

The default supported languages include:

- Chinese (Traditional and Simplified)
- English
- French
- German
- Japanese
- Portuguese
- Russian
- Spanish

The Web-based Manager has three options for applying languages:

- Detect the browser language setting and adjust the display language as appropriate
- Administrator override
- Default system language

Customers will be able to generate their own localized language files. Contact Fortinet Technical Support if you required the translation pack. Customer generated language files can be submitted for inclusion in future official releases.

Scheduled config backup to FTP/SFTP

Schedule a regular backup of the configuration from the FortiAuthenticator unit to an external FTP or SFTP server. Both primary and secondary servers are supported.

Authentication

Authentication covers all of the explicit authentication options within the FortiAuthenticator system, including: RADIUS, LDAP, Two-Factor, EAP, guest management, and user self-service features.

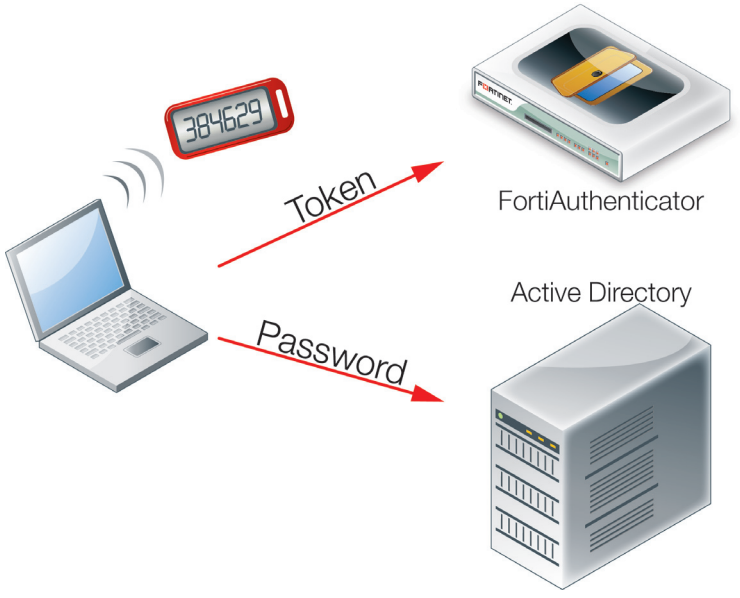
FortiAuthenticator Agent for Microsoft Windows

FortiAuthenticator supports two factor authentication with methods such as RADIUS and LDAP. As it is not possible to replace the authentication process for Microsoft Windows Domain authentication, Fortinet has introduced the Two Factor Authentication Plugin Module to enhance the existing domain login process.

FortiAuthenticator Agent for Microsoft Windows utilizes the Credential Provider Plugin system provided by Microsoft to add Token Passcode validation to the standard username and password authentication process.

This Agent allows the Username and Password to be validated directly with Active Directory while the Token Passcode is validated through an HTTPS connection to the FortiAuthenticator.

Figure 2: Windows Agent



FortiAuthenticator Agent for Microsoft Windows supports a range of features, including:

- Fail open/closed when the FortiAuthenticator unit is unavailable
- Administrator override
- Login with administrators One-Time Passcode
- Exempted accounts
- Support for password changes
- CLI based configuration to simplify GPO roll outs
- Limit the domains for which a One-Time Passcode is required.

Figure 3: Agent login

Supported operating systems

Server Operating Systems	Desktop Operating Systems
Windows Server 2008 DataCenter X86	Windows Vista Ultimate X86
Windows Server 2008 Enterprise X64	Windows Vista Business X64
Windows Server 2008 R2 DataCenter X64	Windows Vista Enterprise X64
Windows Server 2008 R2 Enterprise X64	Windows 7 Professional X86
Windows Server 2012 Standard X64	Windows 7 Ultimate X64
Windows Server 2012 DataCenter X64	Windows 7 Enterprise X64
	Windows 8 Professional X64
	Windows 8 Enterprise X64

Microsoft Windows 8 x86 standard is unsupported as it is cannot be connected to the domain.

Microsoft Windows XP is not currently supported as it will soon reach end of support with Microsoft. Please contact your Fortinet Account Manager if this is an issue.

User expiration

Previously, user account expiry could only be set for users registering with the self-registration portal and, once set, could not be modified. The ability to configure and modify user account expiry has been extended to the user management interface. See “Adding a user” on page 72.

User lockout

Two enhancements to the user lockout facility have been implemented:

- Permanent lockout on multiple failed attempts: Extends the existing temporary lockout feature by requiring administrator unlock.
- Lockout on user inactivity: Monitor for unused accounts to allow the recovery of dormant accounts.

See “Lockouts” on page 67 for more information.

Guest portal enhancements

The FortiAuthenticator guest self-registration portal allows service providers to allow open access to networks, such as free WiFi in hotels or shops, on the basis that the user must register first. This registration can either be accepted automatically and the user provided with login credentials, or can be sent to an administrator for approval.

With FortiAuthenticator v3.0, a range of new features have been added to allow customization of the registration portal:

- Ability to remove the requirement for Username and use mobile number provided

  Allows the login credentials to be sent in a text message to the user as a guarantee of identity for compliance purposes.
- Customization of the fields which are displayed on the self-registration page

  Allows organizations to tailor the information collected from their customers based on business needs.
- Customizable HTML for the self-registration page
  - HTML can be fully customized to match the corporate look and feel, and to add custom messages.
  - Images and content/frames/adverts can be pulled in from external sources.
  - Images can be uploaded and directly served from the FortiAuthenticator.

Replacement messages

The concept of replacement messages has been added. This gives an administrator full control over the content displayed to the end user in a variety of interfaces, including:

- E-mail Token Message
- E-mail Token Subject
- User Registration Receipt Message (via e-mail or browser)
- User Registration Receipt Message (via SMS)
- Login Page
- Token Login Page
- Password Reset Complete Page
- Password Reset E-mail Instruction Page
- Password Set Complete Page
- User Registration Confirmation Page (with Admin Approval)
- SMS Verification Page
- User Registration Confirmation Page
- Resend Registration Receipt Page
- SMS One-Time Passcode Message
- User Registration Page.

See"Replacement message" on page 93 for more information.

User device certificate self-enrolment

Traditionally, certificate management has been considered complicated. FortiAuthenticator simplifies the creation, signing, management, and distribution of certificates using Simple Certificate Enrollment Protocol (SCEP).

FortiAuthenticator v3.0 further simplifies the user management process by introducing user device self-enrolment. This feature allows end-users to log into the FortiAuthenticator user portal and create certificates for their devices, which can be used in things like BYOD wireless authentication.

User self service certificate enrolment is supported for specific devices using the following protocols and methodologies:

- iPhone/iPad to Automated SCEP via Mobile Config
- Android to Manual PKCS#12
- Windows to PKCS#10 CSR
- Other to SCEP, PKCS#10 CSR, Manual PKCS#12

User management API

To enable integration of the FortiAuthenticator with third party portals and other systems, the API has been extended to enable programmatic user management. This allows for the creation and deletion of users and groups, and the assignment of users to groups.

Self-registration user group

A group can be selected in which to place all self-registered users into after self-registration. This prevents self-registration users from being accidentally included on other user policies on shared systems.

Fortinet Single Sign-On

FSSO is a method used by FortiGate and FortiCache to transparently identify users on the network. See “Fortinet Single Sign-On” on page 112 for more information.

FortiAuthenticator uses both transparent and non-transparent methods to gather user login status information from a variety of disparate locations. It then consolidates and embellishes the information before supplying it to the FortiGate or FortiCache devices for use in identity based policies.

The previous methods of gathering user identities include:

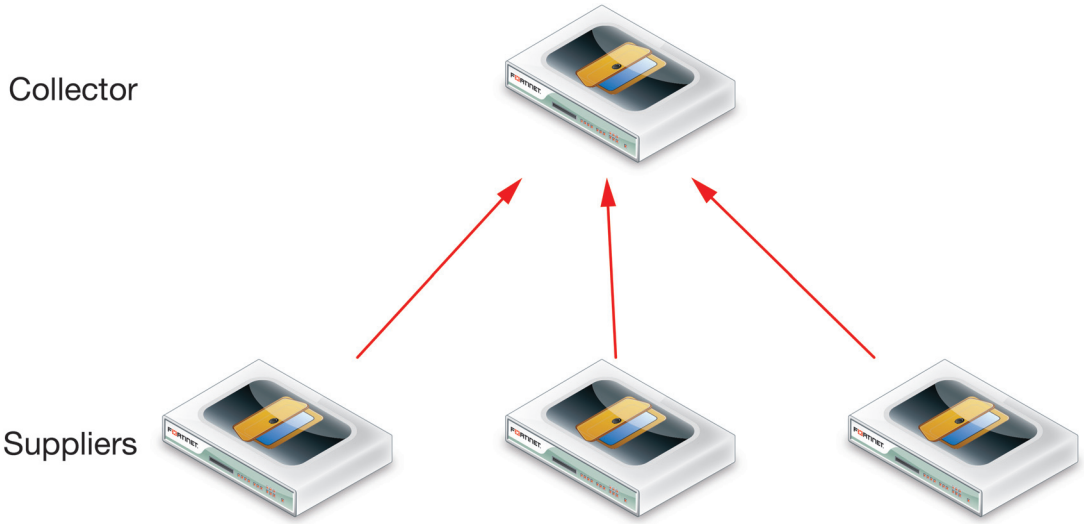
- FortiAuthenticator Portal Login (manual login)
- FortiAuthenticator Portal Login with home page widgets (partially transparent)
- FortiAuthenticator Single Sign On Mobility Agent (transparent)
- Active Directory Polling (transparent)
- RADIUS Accounting (transparent)

FortiAuthenticator v3.0 adds a range of new FSSO functionality.

Hierarchical tiering for DC polling

Tiering of collectors and suppliers allows for the large scale deployment of regional systems performing detection of user identification. It also allows local LDAP group lookup and distribution of events to top level collectors, which then distribute login events to FortiGate and FortiCache devices. See “Fortinet Single Sign-On” on page 112.

Figure 4: Tiering collectors and suppliers

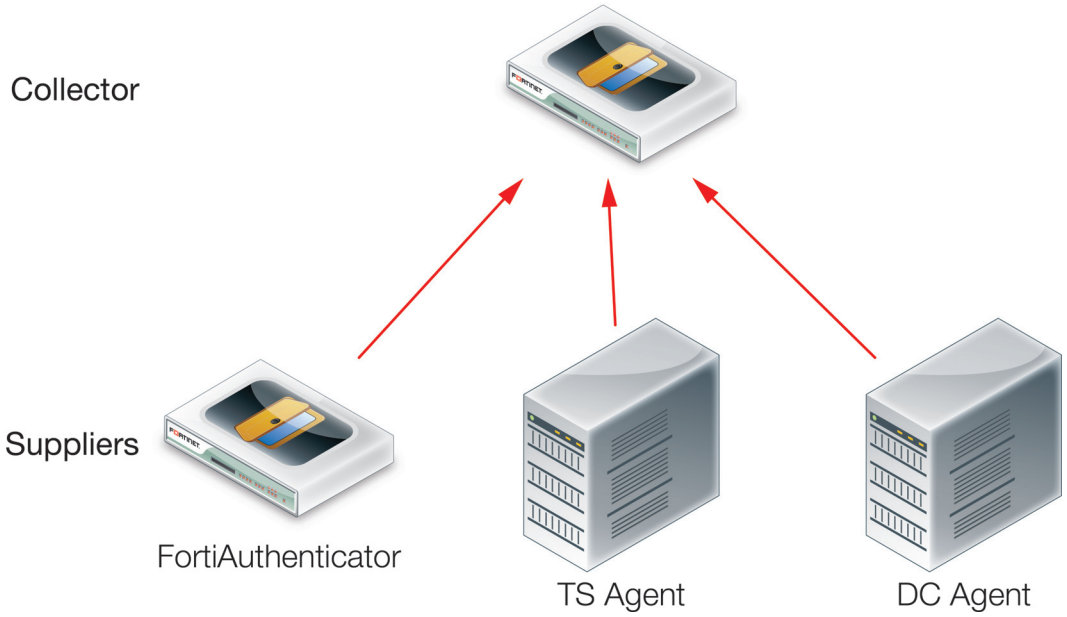


Support DC and TS agents

FortiGate support the concept of DCAgent software for the collection of login information from Windows Active Directory systems through either polling or installation on the domain controller. TSAgent is a similar concept, except it collects user login information from Citrix or Windows Terminal Servers.

FortiAuthenticator implements the polling functionality directly, however, it also accepts a feed from both DCAgent and TSAgent installations if necessary.

Figure 5: DC and TS agents



FSSO exclude users

Service accounts (AV and other software) in a Microsoft Windows environment can cause ghost logins that overwrite valid login. Exclusions allow such service accounts to be ignored to avoid this issue.

FSSO workstation logoff detection

While detection methods such as Active Directory polling can identify user login events, they are unable to directly detect users logging off. FSSO workstation logoff detection utilizes the WMI protocol to detect if the user is still logged in to the workstation and, if not, the login is removed. It also supports DC Polling, SSO Mobility, and DC and TS Agents (currently not RADIUS Accounting or Portal).

FSSO concurrent user limit

To facilitate a flexible BYOD policy, FortiAuthenticator v3.0 introduces the ability to restrict the number concurrent devices a single user account can have logged in.

FSSO user licensing has been modified to support this feature.

Version 2.2 and below: 6 users	
User1	192.168.0.1
User1	192.168.0.2
User1	192.168.0.3
User2	192.168.0.4
User2	192.168.0.5
User3	192.168.0.6

Version 3.0 and above: 3 users	
User1	192.168.0.1
	192.168.0.2
	192.168.0.3
User2	192.168.0.4
	192.168.0.5
User3	192.168.0.6

API FSSO Login

The FortiAuthenticator API has been extended to allow third party systems to push FSSO login and logout events into the FortiAuthenticator database. This allows the integration of third party authentication applications and web portals with FSSO

Setup

For information about installing the FortiAuthenticator unit and accessing the CLI or web-based manager, refer to the Quick Start Guide provided with your unit.

This chapter provides basic setup information for getting started with your FortiAuthenticator device. For more detailed information about specific system options, see "System" on page 31.

The following topics are included in this section:

Initial setup

The following section provides information about setting up the Virtual Machine (VM) version of the product.

FortiAuthenticator VM setup

Before using FortiAuthenticator-VM, you need to install the VMware application to host the FortiAuthenticator-VM device. The installation instructions for FortiAuthenticator-VM assume you are familiar with VMware products and terminology.

System requirements

For information on the FortiAuthenticator-VM system requirements, please see the product datasheet available at http://www.fortinet.com/products/fortiauthenticator.

FortiAuthenticator-VM has kernel support for more than 4GB of RAM in VM images. However, this support also depends on the VM player version. For more information, see: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1014006

The default *Hardware Version* is 4 to support the widest base of VM players. However you can modify the VM Hardware Version by editing the following line in the FortiAuthenticator-VM.vmx file:

```
virtualHW.version = "4"
```

FortiAuthenticator-VM image installation and initial setup

The following procedure describes setup on VMware Fusion.

To set up the FortiAuthenticator VM image:

1. Download the VM image ZIP file to the local computer where VMware is installed.
2. Extract the files from the zip file into a folder.
3. In your VMware software, go to *File* > *Open*.

4. Navigate to the expanded VM image folder, select the *FortiAuthenticator-VM.vmx* file and select *Open*.

   VMware will install and start FortiAuthenticator-VM. This process can take a minute or two to complete.
5. At the FortiAuthenticator login prompt, enter `admin` and press Enter.
6. At the password prompt, press Enter. By default, there is no password.
7. At the CLI prompt enter the following commands:

   ```
   set port1-ip 192.168.1.99/24
   set default-gw 192.168.1.2
   ```

   Substitute your own desired FortiAuthenticator IP address and default gateway.

You can now connect to the Web-based Manager at the IP address you set for port 1.

Suspending the FortiAuthenticator-VM can have unintended consequences. Fortinet recommends that you do not use the suspend feature of VMware. Instead, shut down the virtual FortiAuthenticator system using the Web-based Manager or CLI, and then shut down the virtual machine using the VMware console.

Administrative access

Administrative access is enabled by default on port 1. Using the Web-based Manager, you can enable administrative access on other ports if necessary.

To add administrative access to an interface:

1. Go to *System* > *Network* > *Interfaces* and select the interface you need to add administrative access to. See “Interfaces” on page 42.
2. In *Admin access*, select the types of access to allow. See “Admin access” on page 43.
3. Select *OK*.

Web-based Manager access

To use the Web-based Manager, point your browser to the IP address of port 1 (192.168.1.99 by default). For example, enter the following in the URL box:

```
https://192.168.1.99
```

Enter `admin` as the *User Name* and leave the *Password* field blank.

HTTP access is not enabled by default. To enable access, use the `set ha-mgmt-access` command in the CLI (see “CLI commands” on page 27), or enable HTTP access on the interface in the Web-based Manager (see “Interfaces” on page 42).

Telnet

CLI access is available using telnet to the port1 interface IP address (192.168.1.99 by default). Use the telnet -K option so that telnet does not attempt to log on using your user ID. For example:

```
$ telnet -K 192.168.1.99
```

At the FortiAuthenticator login prompt, enter `admin`. When prompted for password press `Enter`. By default there is no password. When you are finished, use the `exit` command to end the telnet session.

CLI access using Telnet is not enabled by default. To enable access, use the `set ha-mgmt-access` command in the CLI (see "CLI commands" on page 27), or enable Telnet access on the interface in the Web-based Manager (see "Interfaces" on page 42).

SSH

SSH provides secure access to the CLI. Connect to the port1 interface IP address (192.168.1.99 by default). Specify the user name `admin` or SSH will attempt to log on with your user name. For example:

```
$ ssh admin@192.168.1.99
```

At the password prompt press `Enter`. By default there is no password. When you are finished, use the `exit` command to end the session.

Adding a FortiAuthenticator unit to your network

Before setting up the FortiAuthenticator unit, there are some requirements for your network:

- You must have security policies that allow traffic between the client network and the subnet of the FortiAuthenticator,
- You must ensure that the following ports are open in the security policies between the FortiAuthenticator and authentication clients, in addition to management protocols such as HTTP, HTTPS, telnet, SSH, ping, and other protocols you may choose to allow:
  - UDP/161 (SNMP)
  - UDP/1812 (RADIUS Auth)
  - UDP/1813 (RADIUS Accounting)
  - TCP/389 (LDAP)
  - TCP/636 (LDAPS)
  - TCP/8000 (FortiGate FSSO)
  - TCP/80 (OCSP)
  - TCP/8001 (FortiClient FSSO)
  - TCP/8002 (DC/TS Agent FSSO)
  - TCP/8003 (Hierarchical FSSO)

To setup FortiAuthenticator on your network:

1. Log on to the Web-based Manager.

   Username: `admin`, no password.
2. Go to *System* > *Network* > *DNS*. Enter your internal network primary and secondary name server IP addresses. This is essential for successful FSSO operation. See "DNS" on page 44
3. Go to *System* > *Network* > *Static Routing* and create a default route (IP/Mask 0.0.0.0/0) to your network gateway on the interface that connects to the gateway. See "Static Routing" on page 44.
4. Go to System > *Dashboard* > *Status*.
5. In the *System Information* widget select *Change* in the *System Time* field, then select your time zone from the list.
6. Either enable the NTP, or manually enter the date and time. See "Configuring the system time, time zone, and date" on page 36.

   Enter a new time and date by either typing it manually, selecting *Today* or *Now*, or select the calendar or clock icons for a more visual method of setting the date and time.

If you will be using FortiToken devices, Fortinet strongly recommends using NTP. FortiToken Time based authentication tokens are dependent on an accurate system clock.

7. Select *OK*.
8. If the FortiAuthenticator is connected to additional subnets, configure additional FortiAuthenticator interfaces as required. See "Interfaces" on page 42.

Maintenance

System maintenance tasks include:

- Backing up the configuration
- Upgrading the firmware
- Licensing

Backing up the configuration

You can back up the configuration of the FortiAuthenticator unit to your local computer. The backup file is encrypted to prevent tampering. This configuration file backup includes both the CLI and Web-based Manager configurations of the FortiAuthenticator unit. The backed-up information includes users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP, and certificates. See "Backing up and restoring the configuration" on page 37 for more information.

Automatic system configuration backup can also be configured. See "Config Auto-backup" on page 48 for information.

To back up your configuration

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Backup/Restore*.
3. Under *Backup*, select *Download backup file* and save the file on your computer.

To restore your configuration

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Backup/Restore*.
3. Under *Restore*, select *Browse...*, locate the backup file on your computer, and then select *Restore*.

   You will be prompted to confirm the restore action. The FortiAuthenticator unit will reboot.

When you restore the configuration from a backup file, any information changed since the backup will be lost. Any active sessions will be ended and must be restarted. You will have to log back in when the system reboots.

Upgrading the firmware

Periodically, Fortinet issues firmware upgrades that fix known issues, add new features and functionality, and generally improve your FortiAuthenticator experience. See “Firmware” on page 48 for more information.

Before proceeding to upgrade your system, Fortinet recommends you back up your configuration. Please follow the procedure detailed in “Backing up the configuration” on page 25.

To upgrade the firmware, you must first register your FortiAuthenticator with Fortinet. See “Registering your Fortinet product” on page 13.

To upgrade FortiAuthenticator firmware:

1. Download the latest firmware to your local computer from the Fortinet Technical Support web site, https://support.fortinet.com.
2. Go to *System* > *Administration* > *Firmware*.
3. Select *Browse...*, and locate the firmware image on your local computer.
4. Select *OK*.

   When you select *OK*, the firmware image will upload from your local computer to the FortiAuthenticator device, which will then reboot. You will experience a short period of time during this reboot when the FortiAuthenticator device is offline and unavailable for authentication.

Licensing

FortiAuthenticator-VM works in evaluation mode until it is licensed. The license is valid only if one of the FortiAuthenticator interfaces is set to the IP address specified in the license. See “Licensing” on page 54 for more information.

To license FortiAuthenticator:

1. Go to *System* > *Administration* > *Licensing*.
2. Select *Browse...* and locate on your local computer the license file you received from Fortinet.
3. Select *OK*.

CLI commands

The FortiAuthenticator has CLI commands that are accessed using SSH, or Telnet. Their purpose is to initially configure the unit, perform a factory reset, or reset the values if the Web-based Manager is not accessible for some reason.

Table 1: General commands

Command	Description
`help`	Display list of valid CLI commands. You can also enter ? for help.
`exit`	Terminate the CLI session.

Table 2: Configuration commands

Command	Description
`set port1-ip <addr_ipv4mask>`	Enter the IPv4 address and netmask for the port1 interface. Netmask is expected in the /xx format, for example `192.168.0.1/24`. Once this port is configured, you can use the web-based manager to configure the remaining ports.
`set default-gw <addr_ipv4>`	Enter the IPv4 address of the default gateway for this interface. This is the default route for this interface.
`set date <YYYY-MM-DD>`	Enter the current date. Valid format is four digit year, 2 digit month, and 2 digit day. For example: `set date 2014-08-12` sets the date to August 12th, 2014.
`set time <HH:MM:SS>`	Enter the current time. Valid format is two digits each for hours, minutes, and seconds. 24-hour clock is used. For example 15:10:00 is 3:10pm.
`set tz <timezone_index>`	Enter the current time zone using the time zone index. To see a list of index numbers and their corresponding time zones, enter `set tz ?`.
`set ha-mode {enable | disable}`	Enable or disable (default) HA mode.
`set ha-port <interface>`	Select a network interface to use for communication between the two cluster members. This interface must not already have an IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
`set ha-priority {high | low}`	Set to `Low` on one unit and `High` on the other. Normally, the unit with High priority is the master unit.

Table 2: Configuration commands (continued)

Command	Description
`set ha-mgmt-ip <ip4_addr>`	Enter the IP address, with netmask, that this unit uses for HA related communication with the other FortiAuthenticator unit. Format: 1.2.3.4/24. The two units must have different addresses. Usually, you should assign addresses on the same private subnet.
`set ha-mgmt-access {ssh | https | http | telnet}`	Select the types of administrative access to allow.
`set ha-dbg-level <level>`	Enter the detail level for HA service debug logs. Range: -4 (least verbose) to 4 (most verbose).
`unset <setting>`	Restore default value. For each `set` command listed above, there is an `unset` command, for example `unset port1-ip`.

Table 3: System commands

Command	Description
`show`	Display current settings of port1: IP address, netmask, default gateway, and time zone.
`hardware-info`	Show hardware related information.
`ha-rebuild`	Rebuild the configuration database from scratch using the HA peer's configuration.
`restore-admin`	Restore factory reset's admin access settings to the port1 network interface.
`reboot`	Perform a hard restart of the FortiAuthenticator unit. All sessions will be terminated. The unit will go offline and there will be a delay while it restarts.
`factory-reset`	Enter this command to reset the FortiAuthenticator settings to factory default settings. This includes clearing the user database. This procedure deletes all changes that you have made to the FortiAuthenticator configuration and reverts the system to its original configuration, including resetting interface addresses.
`shutdown`	Turn off the FortiAuthenticator.
`status`	Display basic system status information including firmware version, build number, serial number of the unit, and system time.

Table 4: Diagnostic commands

Command	Description
`hardware-info`	Display general hardware status information.
`disk-attributes`	Display system disk attributes.
`disk-errors`	Display any system disk errors.
`disk-health`	Display disk health information.
`disk-info`	Display disk hardware status information.
`raid-hwinfo`	Display RAID hardware status information.

Table 5: Utilities

Command	Description
`nslookup`	Basic tool for DNS debugging.
`dig`	Advanced DNS debugging.
`ping`	Test network connectivity to another network host.
`tcpdump`	Examine local network traffic.
`traceroute`	Examine the route taken to another network host.

Troubleshooting

Troubleshooting includes useful tips and commands to help deal with issues that may occur. For additional help, contact customer support. See “Troubleshooting” on page 163 for more information.

If you have issues when attempting authentication on a FortiGate unit using the FortiAuthenticator, there are some FortiAuthenticator and FortiGate settings to check.

In addition to these settings you can use log entries, monitors, and debugging information to determine more information about your authentication problems. For help with FortiAuthenticator logging, see “Logging” on page 157. For help with FortiGate troubleshooting, see the *FortiOS Handbook Troubleshooting and User Authentication guides chapters*.

FortiAuthenticator settings

When checking FortiAuthenticator settings, you should ensure:

- there is an authentication client entry for the FortiGate unit. See "Adding a RADIUS authentication client" on page 97,
- the user trying to authenticate has a valid active account that is not disabled, and that the username and password are spelled correctly,
- the user account allows RADIUS authentication if RADIUS is enabled on the FortiGate unit,
- the FortiGate unit can communicate with the FortiAuthenticator unit, on the required ports:

  RADIUS Authentication: UDP/1812

  LDAP: TCP/389
- the user account exists
  - as a local user on the FortiAuthenticator (if using RADIUS authentication),
  - in the local LDAP directory (if using local LDAP authentication),
  - in the remote LDAP directory (if using RADIUS authentication with remote LDAP password validation),
- the user is a member in the expected user groups and these user groups are allowed to communicate on the authentication client (the FortiGate unit, for example),
- If authentication fails with the log error *bad password*, try resetting the password. If this fails, verify that the pre-shared secret is identical on both the FortiAuthenticator unit and the authentication client.

If FortiToken authentication is failing, try the following:

- Verify that the token is correctly synchronized.
- Remove the token from the user authentication configuration and verify authentication works when the token is not present.
- Attempt to log into the FortiAuthenticator with the user credentials.

These steps enable the administrator to identify whether the problem is with the FortiGate unit, the credentials or the FortiToken.

FortiGate settings

When checking FortiGate authentication settings, you should ensure

- the user has membership in the required user groups and identity-based security policies,
- there is a valid entry for the FortiAuthenticator device as a remote RADIUS or LDAP server,
- the user is configured either explicitly or as a wildcard user.

System

The *System* tab enables you to manage and configure the basic system options for the FortiAuthenticator unit. This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the device, and managing messaging servers and services.

The *System* tab provides access to the following menus and sub-menus:

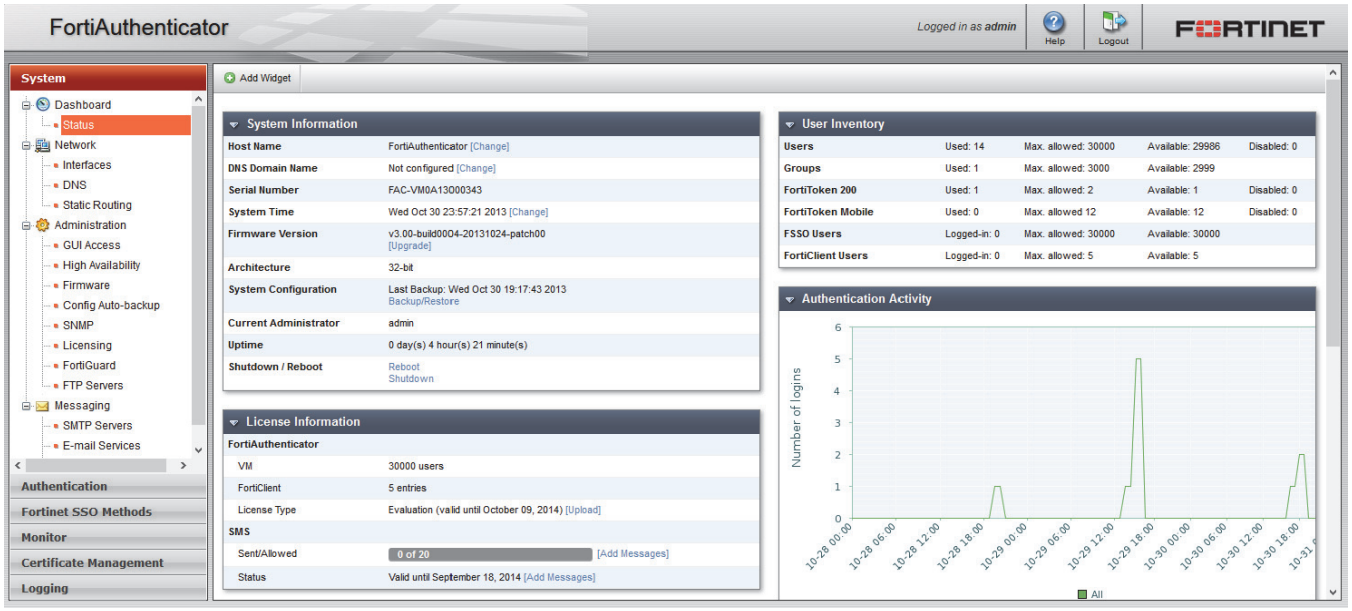
Dashboard	Select this menu to monitor, and troubleshoot your FortiAuthenticator device. Dashboard widgets include: • System Information • System Resources • Authentication Activity • User Inventory • HA Status • License Information • Disk Monitor • Top User Lockouts
Network	Select this menu to configure your FortiAuthenticator interfaces and network settings. • Interfaces • DNS • Static Routing
Administration	Select this menu to configure administrative settings for the FortiAuthenticator device. • GUI Access • High Availability • Firmware • Config Auto-backup • SNMP • Licensing • FortiGuard • FTP Servers
Messaging	Select this menu to configure messaging servers and services for the FortiAuthenticator device. • SMTP Servers • E-mail Services • SMS Gateways

Dashboard

When you select the *System* tab, it automatically opens at the *System* > *Dashboard* page.

The *Dashboard* page displays widgets that provide performance and status information and enable you to configure some basic system settings. These widgets appear on a single dashboard.

Figure 6: FortiAuthenticator system dashboard



The following widgets are available:

System Information	Displays basic information about the FortiAuthenticator system including host name, DNS domain name, serial number, system time, firmware version, architecture, system configuration, current administrator, and up time. From this widget you can manually update the FortiAuthenticator firmware to a different release. For more information, see "System Information widget" on page 34.
System Resources	Displays the usage status of the CPU and memory. For more information, see "System Resources widget" on page 38.
Authentication Activity	Displays a customizable graph of the number of logins to the device. For more information, see "Authentication Activity widget" on page 39.
User Inventory	Displays the numbers of users, groups, FortiTokens, FSSO users, and FortiClient users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled. For more information, see "User Inventory widget" on page 40.
HA Status	Displays whether or not HA is enabled.
License Information	Displays the devices license information, as well as SMS information. For more information, see "License Information widget" on page 40.

Disk Monitor	Displays if RAID is enabled, and the current disk usage in GB.
Top User Lockouts	Displays the top user lockouts. For more information, see "License Information widget" on page 40.

Customizing the dashboard

The FortiAuthenticator system settings dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

To move a widget

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To add a widget

In the dashboard toolbar, select *Add Widget*, then select the name of widget that you want to show. Multiple widgets of the same type can be added. To hide a widget, in its title bar, select the *Close* icon.

Figure 7: Add a widget dialog box

To see the available options for a widget

Position your mouse cursor over the icons in the widget's title bar. Options include show/hide the widget, edit the widget, refresh the widget content, and close the widget.

Figure 8: Widget title bar

The following table lists the widget options.

Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
Edit	Select to change settings for the widget. This option appears only in certain widgets.

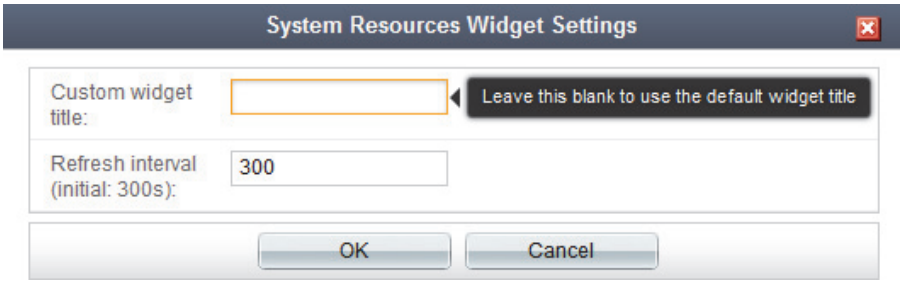
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

To change the widget title

Widget titles can be customized by selecting the edit button in the title bar and entering a new title in the widget settings dialog box. Some widgets have more options in their respective settings dialog box.

To reset a widget title to its default name, simply leave the *Custom widget title* field blank.

Figure 9: Generic widget settings dialog box

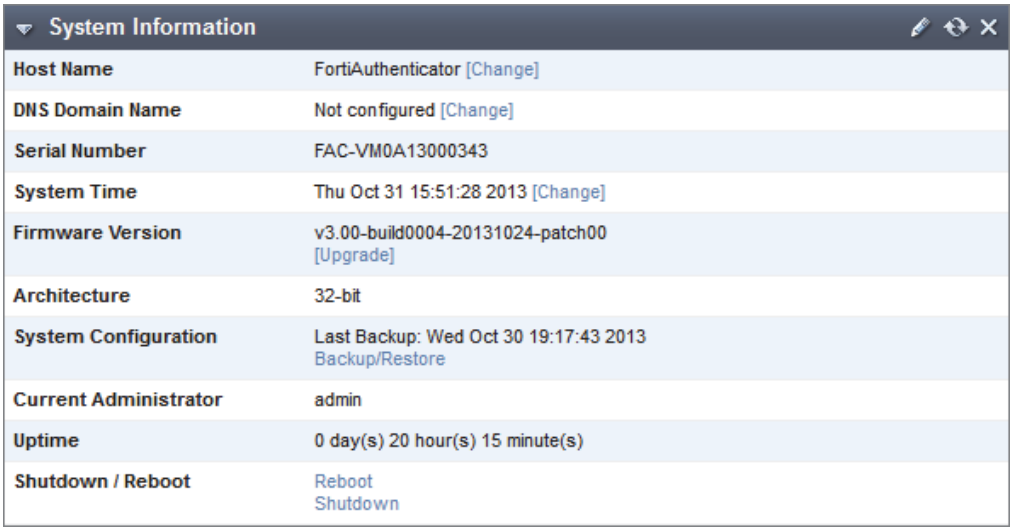


The widget refresh interval can also be manually adjusted from this dialog box.

System Information widget

The system dashboard includes a *System Information* widget, shown in Figure 10, which displays the current status of the FortiAuthenticator unit and enables you to configure basic system settings.

Figure 10: System information widget



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAuthenticator unit. For more information, see "Changing the host name" on page 35.
DNS Domain Name	The DNS domain name. For more information, see "Changing the DNS domain name" on page 36.
Serial Number	The serial number of the FortiAuthenticator unit. The serial number is unique to the FortiAuthenticator unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
System Time	The current date, time, and time zone on the FortiAuthenticator internal clock or NTP server. For more information, see "Configuring the system time, time zone, and date" on page 36.
Firmware Version	The version number and build number of the firmware installed on the FortiAuthenticator unit. To update the firmware, you must download the latest version from the Customer Service & Support portal at https://support.fortinet.com. Select *Update* and select the firmware image to load from your management computer.
Architecture	The architecture of the device, such as 32-bit.
System Configuration	The date of the last system configuration backup. Select Backup/Restore to backup or restore the system configuration. For more information, see "Backing up and restoring the configuration" on page 37.
Current Administrator	The name of the currently logged on administrator.
Uptime	The duration of time the FortiAuthenticator unit has been running since it was last started or restarted.
Shutdown/Reboot	Options to shutdown or reboot the device. When rebooting or shutting down the system, you have the option to enter a message that will be added to the event log explaining the reason for the shutdown or reboot.

Changing the host name

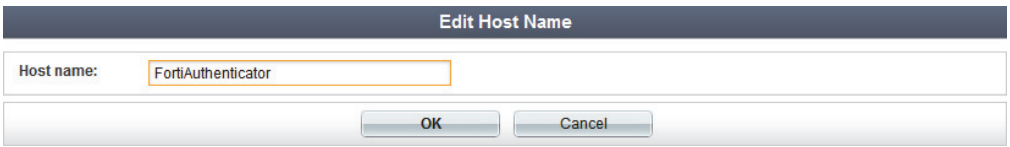
The *System Information* widget will display the full host name.

To change the host name:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *Host Name* field, select *Change*.

   The *Edit Host Name* page opens.

Figure 11: Edit host name



3. In the *Host name* field, type a new host name.

   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Select *OK* to save the setting.

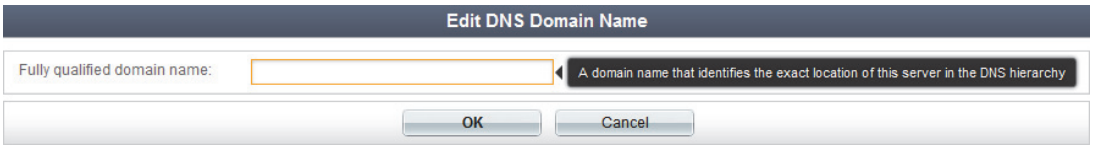
Changing the DNS domain name

To change the DNS domain name:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *DNS Domain Name* field, select *Change*.

   The *Edit DNS Domain Name* page opens.

   Figure 12: Edit DNS domain name



3. Type a DNS domain name in the field.

   The DNS domain name identifies the exact location of this server in the DNS hierarchy.
4. Select *OK* to save the setting.

Configuring the system time, time zone, and date

You can either manually set the FortiAuthenticator system time and date, or configure the FortiAuthenticator unit to automatically keep its system time correct by synchronizing with a NTP server.

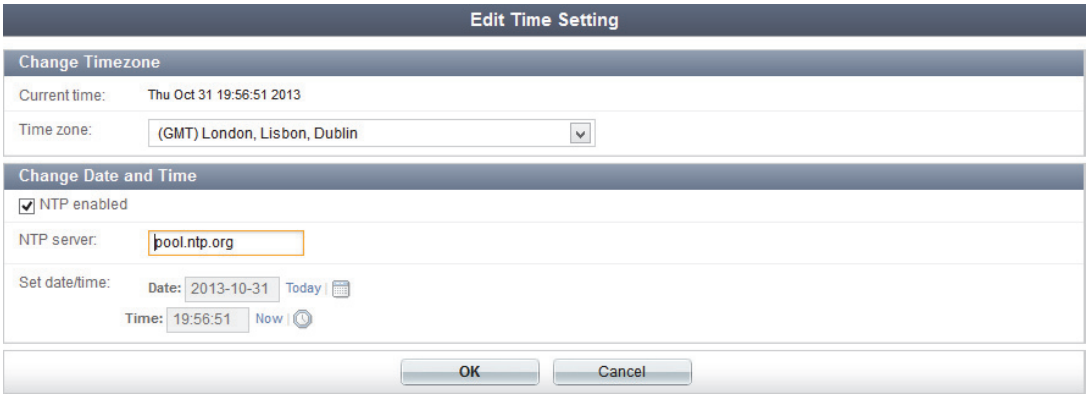
For many features to work the FortiAuthenticator system time must be accurate.

To configure the date and time:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*.

   The *Edit System Time Settings* dialog box appears.

Figure 13: Edit the system time



3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiAuthenticator unit's clock with an NTP server:

Change Timezone	View the current time in the *Current time* field, and select the timezone from the *Time zone* drop-down list.
NTP enabled	Select this option to automatically synchronize the date and time of the FortiAuthenticator unit's clock with an NTP server, then configure the *NTP server* field before you select *OK*. NTP is critical for the time to be accurate and stable for the TOTP method used in two-factor authentication to function correctly.
NTP server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org.
Set date/time	If NTP is not enabled, manually enter the date and time in the appropriate fields. You can also select the calendar or clock icons to select a specific date or general time from the pop-up menus.

4. Select *OK* to apply your changes.

Backing up and restoring the configuration

Fortinet recommends that you back up your FortiAuthenticator configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal affect to the network. You should also perform a back up after making any changes to the FortiAuthenticator configuration.

You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiAuthenticator unit before upgrading the FortiAuthenticator firmware.

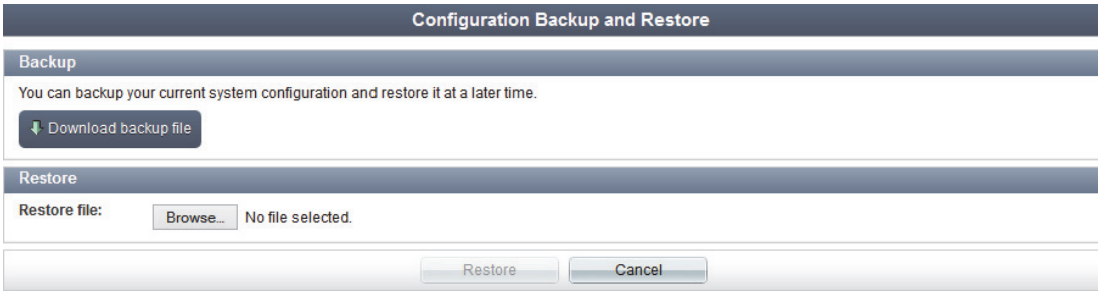
your FortiAuthenticator configuration can also be restored from a backup file on your management computer.

To backup or restore the FortiAuthenticator configuration:

1. Go to *System* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Backup/Restore*.

   The *Configuration Backup and Restore* page appears.

Figure 14: Configuration backup and restore page



3. Select from the following settings:

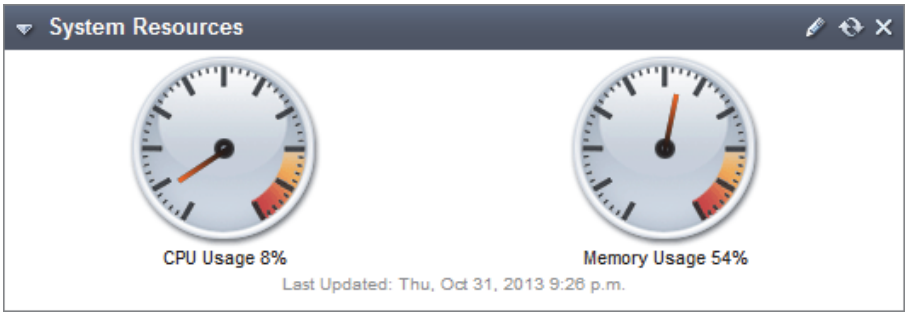
Download backup file	Select *Download backup file* to save a backup file onto the management computer.
Restore File	Select *Browse...* to find the backup file on your management computer, then select *Restore* to restore the selected backup configuration to the device.

4. Select *Cancel* to return to the dashboard page.

System Resources widget

The *System Resources* widget on the dashboard displays the usage status of the CPU and memory as a percentage.

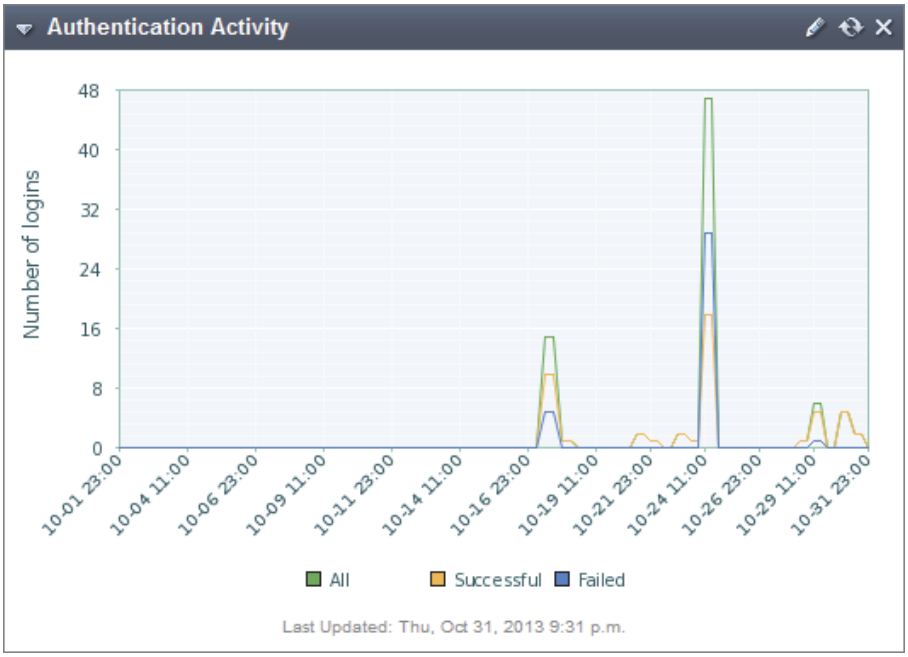
Figure 15: System resources widget



Authentication Activity widget

The *Authentication Activity* widget displays a line graph of the number of logins versus time.

Figure 16: Authentication activity widget



To adjust the data displayed in the graph, select the edit button to open the *Authentication Activity Widget Settings* dialog box.

Figure 17: Authentication activity widget settings

The following settings are available:

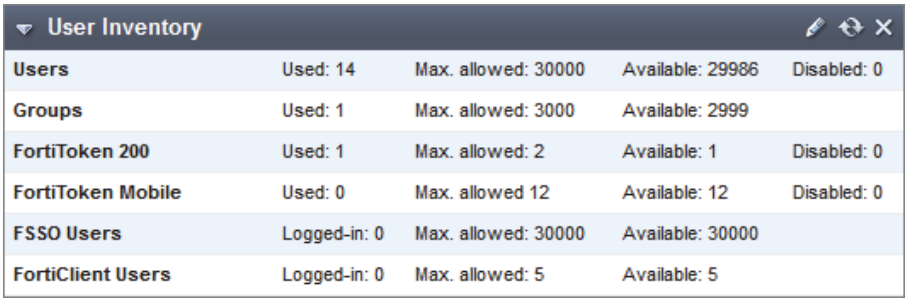
Custom widget title	Enter a custom widget title for the widget, or leave it blank to keep the default title.
Refresh interval	Enter a custom refresh interval for the widget (in seconds), or leave it as the default time of 300 seconds.

Time period	Select a time period for the graph to cover from the drop-down list. The available options are: last 6 hours, last 24 hours, last 3 days, last 7 days, and last 30 days.
Activity Type	Select the activity type to display in the graph. The available options are: All login attempts, Successful login attempts, and Failed login attempts.

User Inventory widget

The *User Inventory* widget displays the numbers of users, groups, FortiTokens, FSSO users, and FortiClient users currently used or logged in, as well as the maximum allowed number, the number still available, and the number that are disabled.

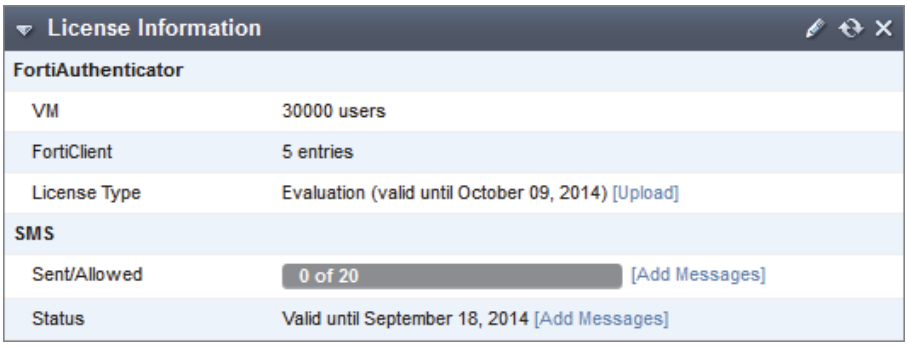
Figure 18: User inventory widget



License Information widget

The *License Information* widget displays the devices license information, as well as SMS information. You can also add a license and more SMS messages.

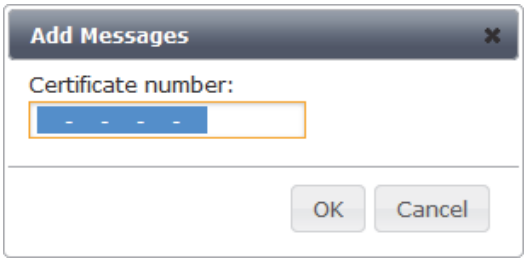
Figure 19: License information widget



To upload a new license file, select *Upload* in the *License Type* field, then browse to the license file on the management computer.

To add more SMS messages, select *Add Messages* from either the *Sent/Allowed* field or the *Status* field. In the *Add Messages* dialog box, enter the certificate number for the messages and then select *OK* to add the messages.

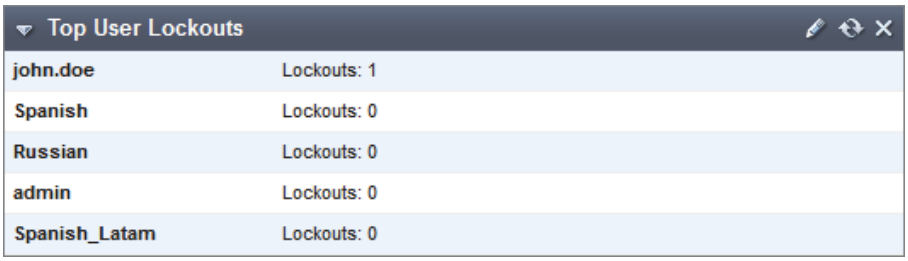
Figure 20: Add messages



Top User Lockouts widget

The *Top User Lockouts* widget displays the users who are locked out the most. For more information on user lockouts and for instruction on adjusting user lockout settings, see "Lockouts" on page 67.

Figure 21: Top user lockouts widget



To change the number of user lockouts displayed in the widget, select the edit icon and change the number in the *Number of lockouts* field.

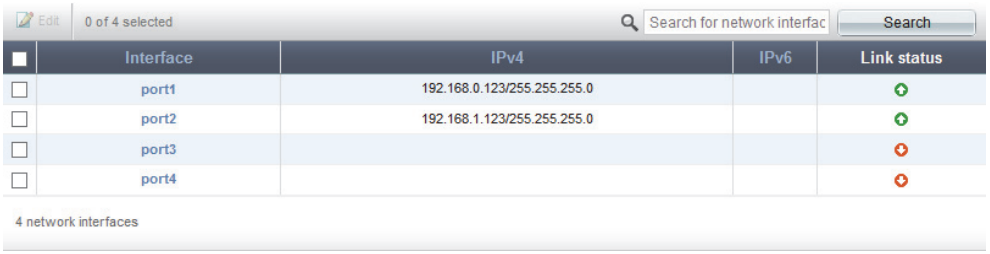
Network

The *Network* tree menu allows you to configure the device interfaces, DNS configuration, and static routing.

Interfaces

To view the interface list, go to *System* > *Network* > *Interfaces*.

Figure 22: Network interfaces



The following information is shown:

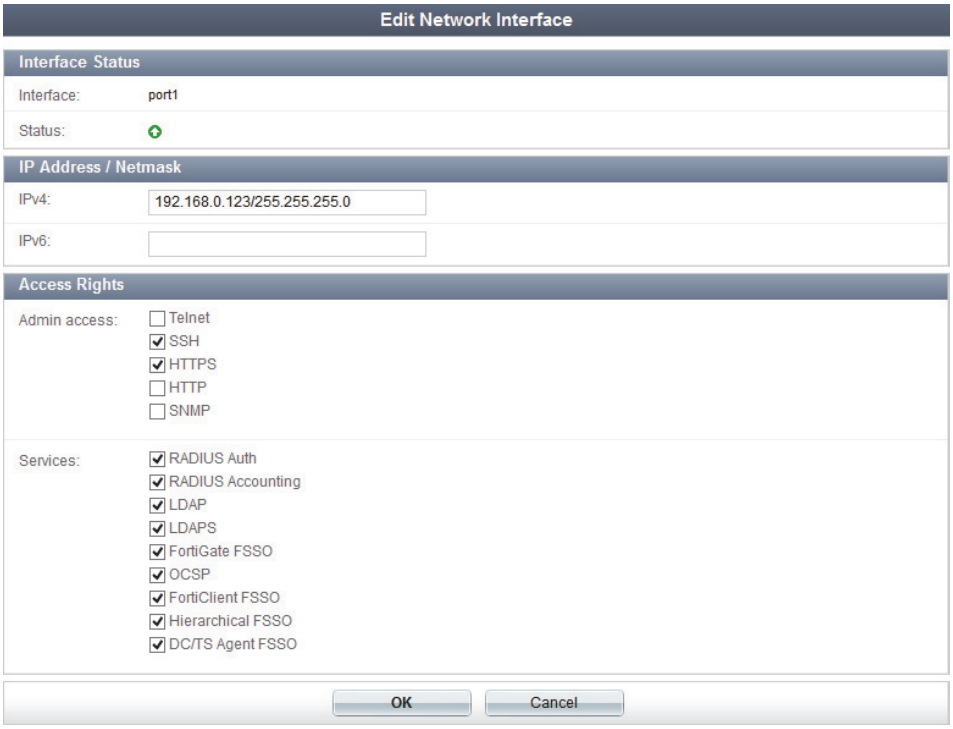
Edit	Select to edit the selected interface. See "To edit an interface:" on page 43 for more information.
Search	Enter a search term in the search text box then select *Search* to search the interface list.
Interface	The names of the physical interfaces on your FortiAuthenticator unit. The name, including number, of a physical interface depends on the model.
IPv4	The IPv4 address of the interface.
IPv6	The IPv6 address of the interface, if applicable.
Link Status	The link status of the interface.

To edit an interface:

1. In the interfaces list, select the interface you need to edit and select the *Edit* button, or select the interface name.

   The *Edit Network Interface* window opens.

   Figure 23: Edit network interface



2. Edit the following settings as required.

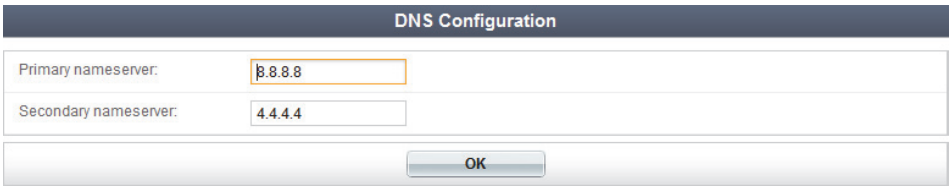
Interface Status	The interface name and it's current link status is displayed.
IP Address / Netmask	
IPv4	Enter the IPv4 address and netmask associated with this interface.
IPv6	Enter the IPv6 address associated with this interface.
Access Rights	
Admin access	Select the allowed administrative service protocols from: *Telnet*, *SSH*, *HTTPS*, *HTTP*, *SNMP*.
Services	Select the allowed services from: *RADIUS Auth*, *RADIUS Accounting*, *LDAP*, *LDAPS*, *FortiGate FSSO*, *OCSP*, *FortiClient FSSO*, *Hierarchical FSSO*, *DC/TS Agent FSSO*.

3. Select *OK* to apply the edits to the network interface.

DNS

To configure DNS settings, go to *System* > *Network* > *DNS*. The primary and secondary nameserver IP addresses can be changed as needed. To apply the changes, select *OK*.

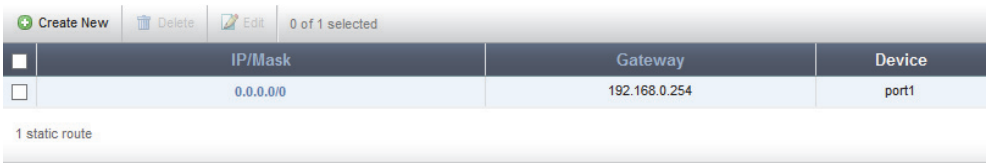
Figure 24:DNS configuration



Static Routing

To view the list of static routes, go to *System* > *Network* > *Static Routing*. Routes can be created, edited, and deleted as required.

Figure 25: Static routing



The following information is shown:

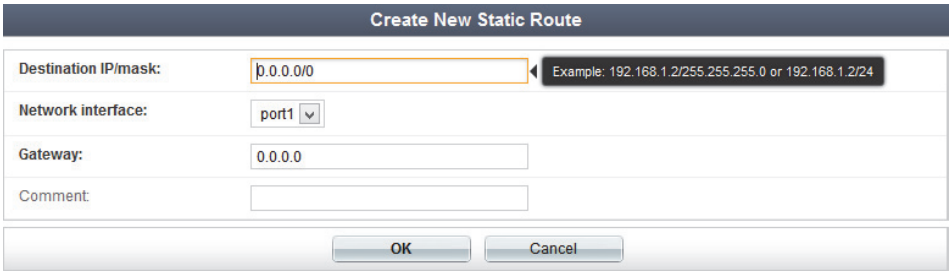
Create New	Select to create a new static route. See "To create a new static route:" on page 45 for more information.
Delete	Select to delete the selected static route. See "To delete a static route:" on page 45 for more information.
Edit	Select to edit the selected static route. See "To edit a static route:" on page 45 for more information.
IP/Mask	The destination IP address and netmask for this route.
Gateway	The IP address of the next hop router to which this route directs traffic.
Device	The device or interface associated with this route.

To create a new static route:

1. In the static route list, select *Create New*.

   The *Create New Static Route* window opens.

Figure 26: New static route



2. Edit the following settings as required.

Destination IP/mask	Enter the destination IP address and netmask for this route.
Network interface	Select the network interface that connects to the gateway.
Gateway	Enter the IP address of the next hop router to which this route directs traffic.
Comment	Optionally, enter a comment about the route. Make it fun.

3. Select OK to create the new static route.

To edit a static route:

1. In the static route list, select the route you need to edit and then select *Edit*, or click on the route.

   The *Edit Static Route* window opens.

2. Edit the settings as required, then select *OK* to apply your changes.

To delete a static route:

1. In the static route list, select the route you need to delete.
2. Select *Delete*, then select *OK* in the confirmation dialog box to delete the route.

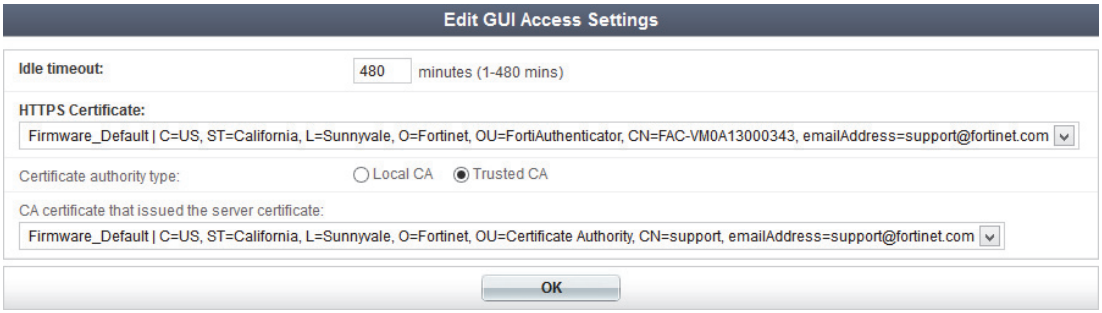
Administration

Configure administrative settings for the FortiAuthenticator device.

GUI Access

To adjust Web-based Manager access settings, go to *System* > *Administration* > *GUI Access*.

Figure 27: Web-based manager access settings



The following settings are available:

Idle timeout	Enter the amount of time before the Web-based Manager times out due to inactivity, from 1 to 480 minutes.
HTTPS Certificate	Select an HTTPS certificate from the drop-down list.
Certificate authority type	Select the selected certificate's authority type, either *Local CA* or *Trusted CA*.
CA certificate that issued the server certificate	Select the issuing server certificate from the drop-down list.

Select *OK* to apply any changes. See "Certificate Management" on page 135 for more information about certificates.

High Availability

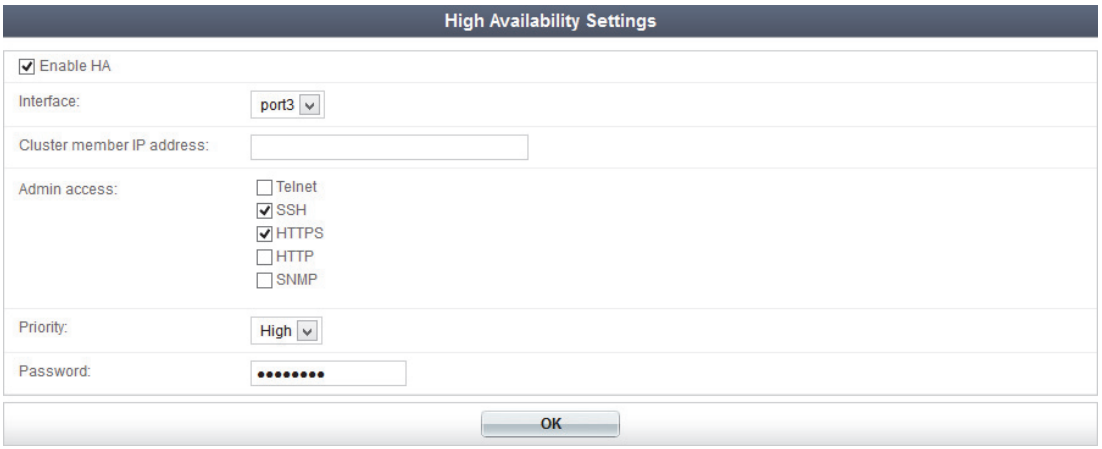
Two FortiAuthenticator units can operate as a cluster to provide even higher reliability, called High Availability (HA). One unit is active and the other is on standby. If the active unit fails, the standby unit becomes active. The cluster is configured as a single authentication server on your FortiGate units.

Authentication requests made during a failover from one unit to another are lost, but subsequent requests complete normally. The failover process takes about 30 seconds.

To configure FortiAuthenticator HA

1. On each unit, go to *System* > *Administration* > *High Availability*

Figure 28: High Availability settings



2. Enter the following information:

Enable HA	Enable HA.
Interface	Select a network interface to use for communication between the two cluster members. This interface must not already have an IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.
Cluster member IP address	Enter the IP address this unit uses for HA-related communication with the other FortiAuthenticator unit. The two units must have different addresses. Usually, you should assign addresses on the same private subnet.
Admin access	Select the types of administrative access to allow from: *Telnet*, *SSH*, *HTTPS*, *HTTP*, and *SNMP*.
Priority	Set to *Low* on one unit and *High* on the other. Normally, the unit with High priority is the master unit.
Password	Enter a string to be used as a shared key for IPsec encryption. This must be the same on both units.

3. Select *OK* to apply the settings.

   When one unit has become the master, reconnect to the Web-based Manager and complete your configuration. The configuration will automatically be copied to the slave unit.

Administrative access to the HA cluster

Administrative access is available through any of the network interfaces using their assigned IP addresses or through the HA interface using the *Cluster member IP address*, assigned on the *System* > *Administration* > *High Availability* page. In all cases, administrative access is available only if it is enabled on the interface.

Administrative access through any of the network interface IP addresses connects only to the master unit. The only administrative access to the slave unit is through the HA interface using the slave unit's *Cluster member IP address*.

Configuration changes made on the master unit are automatically pushed to the slave unit. The slave unit does not permit configuration changes, but you might want to access the unit to change HA settings or for firmware upgrade, shutdown, reboot, or troubleshooting.

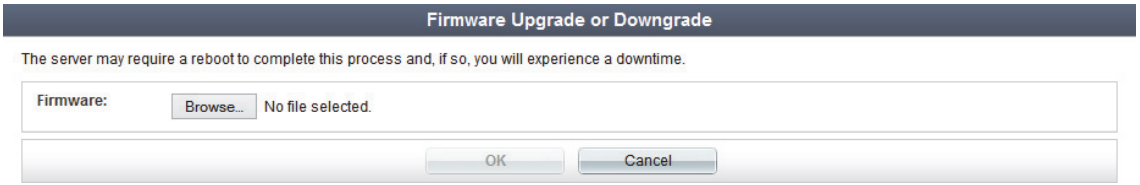
FortiAuthenticator VMs used in an HA cluster each require a license. Each license is tied to a specific IP address. In an HA cluster, all interface IP addresses are the same on the two units, except for the HA interface. Request each license based on either the unique IP address of the unit's HA interface or the IP address of a non-HA interface which will be the same on both units.

If you disable and then re-enable HA operation, the interface that was assigned to HA communication will not be available for HA use. You must first go to *System* > *Network* > *Interfaces* and delete the IP address from that interface.

Firmware

The FortiAuthenticator firmware can be upgraded by either going to *System* > *Administration* > *Firmware*, or through the *System Information* widget of the dashboard (see "System Information widget" on page 34).

Figure 29: Firmware upgrade or downgrade



For instructions on upgrading the device's firmware, see "Upgrading the firmware" on page 26.

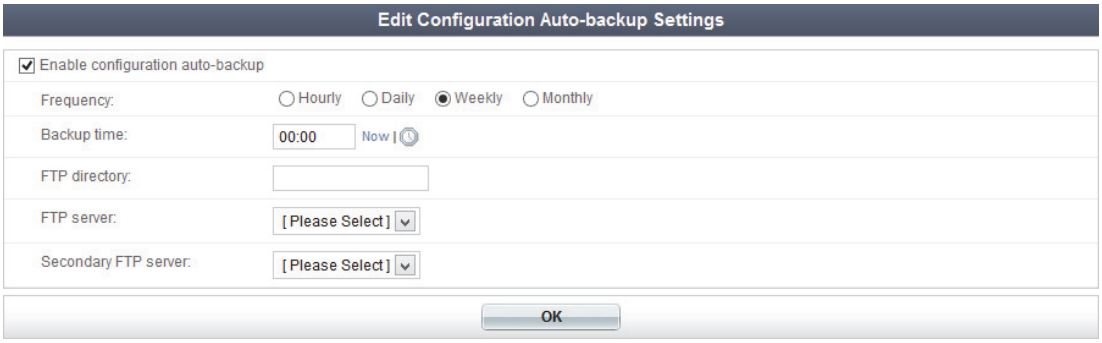
Config Auto-backup

You can configure the FortiAuthenticator to automatically back up the configuration of the FortiAuthenticator unit to an FTP or SFTP server.

Even though the backup file is encrypted to prevent tampering, access to the FTP server should be restricted. This configuration file backup includes both the CLI and Web-based Manager configurations of the FortiAuthenticator unit. The backed-up information includes users, user groups, FortiToken device list, authentication client list, LDAP directory tree, FSSO settings, remote LDAP, and certificates.

To configure automatic backups, go to *System* > *Administration* > *Config Auto-backup*.

Figure 30: Automatic backup configuration



Enter the following information, and then select *OK* to apply the settings:

Enable configuration auto-backup	Enable the configuration of automatic configuration backups.
Frequency	Select the automatic backup frequency, one of: *Hourly*, *Daily*, *Weekly*, or *Monthly*.
Backup time	Entire a time for the backups to occur, or select the clock icon and select from the drop-down menu. You can also select *Now* to set the scheduled time to the current time. This options is not available when the frequency is set to hourly.
FTP directory	Enter the FTP directory where the backup configuration files will be saved.
FTP server	Select the FTP server to which the backup configuration files will be saved.
Secondary FTP server	Select a secondary FTP server.

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiAuthenticator SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is typically a computer running an application that can read the incoming trap and event messages from the agent, and send out SNMP queries to the SNMP agents.

By using an SNMP manager, you can access SNMP traps and data from any FortiAuthenticator interface configured for SNMP management access. Part of configuring an SNMP manager is listing it as a host in a community on the FortiAuthenticator unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that unit, or be able to query that unit.

The FortiAuthenticator SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to system information through queries and can receive trap messages from the FortiAuthenticator unit.

To monitor FortiAuthenticator system information and receive FortiAuthenticator traps, your SNMP manager needs the Fortinet and FortiAuthenticator Management Information Base (MIB) files. A MIB is a text file that lists the SNMP data objects that apply to the device to be monitored. These MIBs provide information that the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiAuthenticator unit SNMP agent.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to important events that occur, such as overuse of memory or a high rate of authentication failures.

SNMP fields contain information about the FortiAuthenticator unit, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

Configuring SNMP

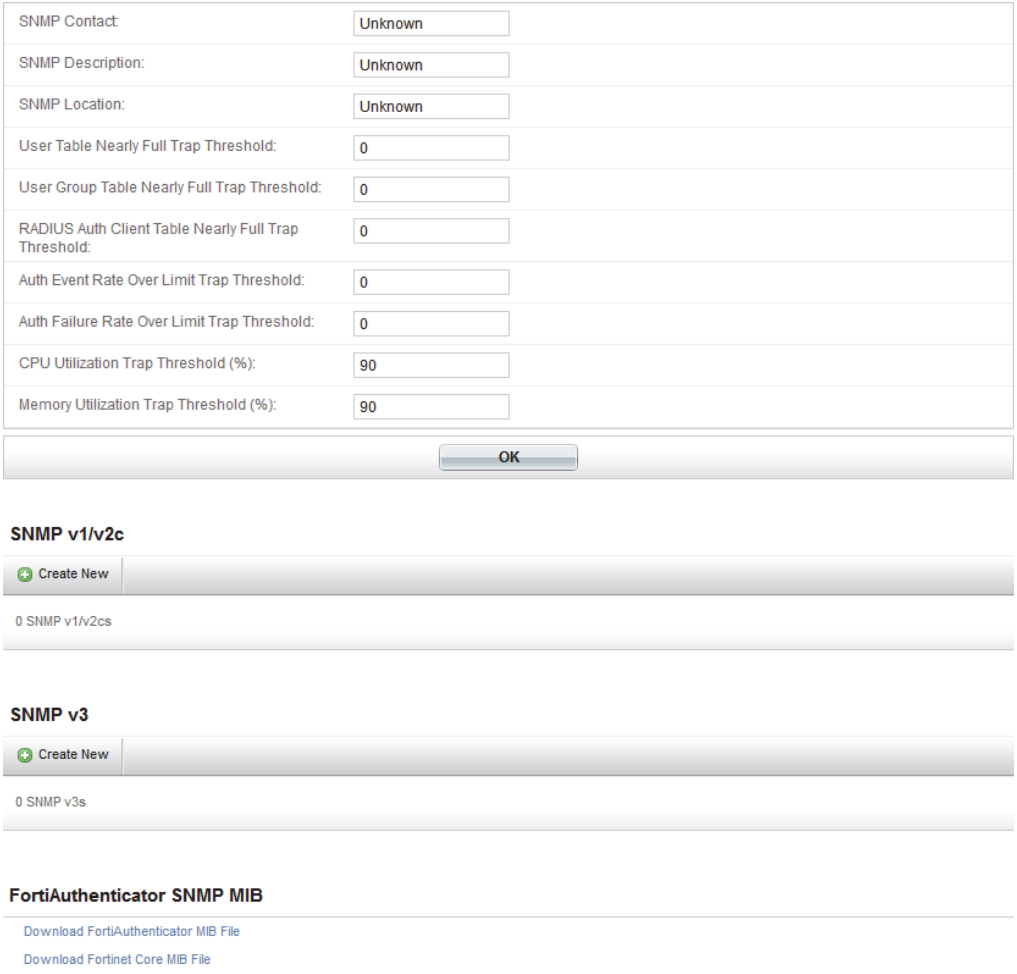
Before a remote SNMP manager can connect to the Fortinet agent, you must configure one or more interfaces to accept SNMP connections by going to *System* > *Network* > *Interfaces*. Select the interface, and in *Administrative Access*, select *SNMP*. See "Interfaces" on page 42.

You can also set the thresholds that trigger various SNMP traps. Note that a setting of zero disables the trap.

To configure SNMP settings:

1. Go to *System* > *Administration* > *SNMP*.

Figure 31:SNMP configuration



2. Enter the following information*:*

SNMP Contact	Enter the contact information for the person responsible for this FortiAuthenticator unit.
SNMP Description	Enter descriptive information about the FortiAuthenticator unit.
SNMP Location	Enter the physical location of the FortiAuthenticator unit.
User Table Nearly Full Trap Threshold	The user table is nearly full. The threshold is a percentage of the maximum permitted number of users.
User Group Table Nearly Full Trap Threshold	The user group table is nearly full. The threshold is a percentage of the maximum permitted number of user groups.
RADIUS Auth Client Table Nearly Full Trap Threshold	The RADIUS authenticated client table is nearly full. The threshold is a percentage of the maximum permitted number of RADIUS clients.
Auth Event Rate Over Limit Trap Threshold	High authentication load. The threshold is the number of authentication events over a 5-minute period.
Auth Failure Rate Over Limit Trap Threshold	High rate of authentication failure. The threshold is the number of authentication failures over a 5-minute period.
CPU Utilization Trap Threshold (%)	High load on CPU. Default 90%.
Memory Utilization Trap Threshold (%)	Too much memory used. Default 90%.

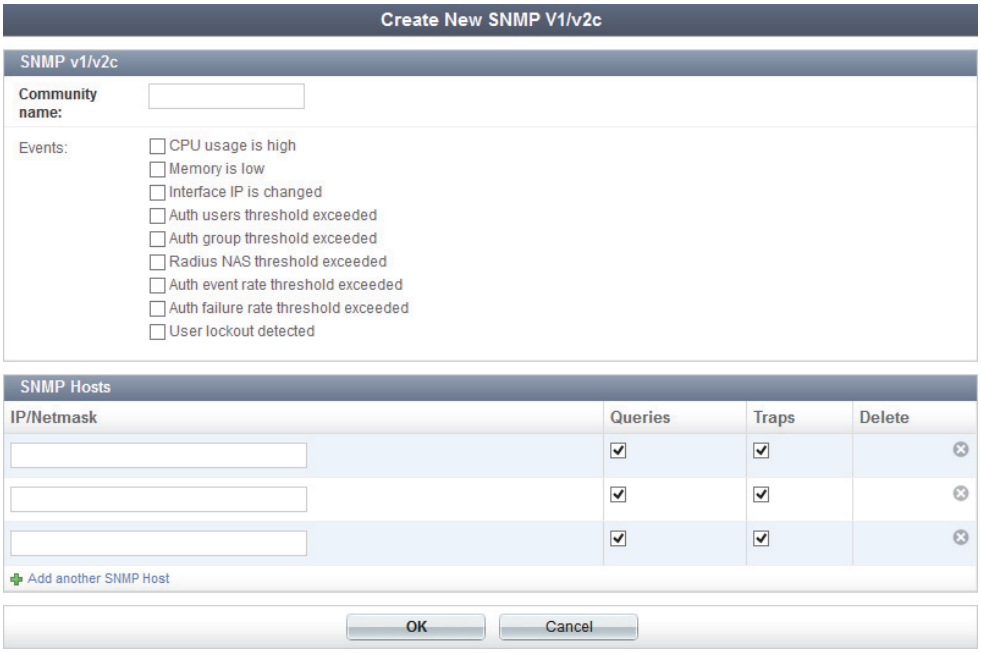
3. Select *OK* to apply the changes.

To create a new SNMP community:

1. Go to *System* > *Administration* > *SNMP.*
2. Select *Create New* under *SNMP v1/v2c*.

   The *Create New SNMP V1/v2c* window opens.

Figure 32: New SNMP V1/V2C



3. Enter the following information in the *SNMPv1/v2c* section:

Community	The name of the SNMP community.
Events	Select the events for which traps are enabled. Options include: • CPU usage is high • Memory is low • Interface IP is changed • Auth users threshold exceeded • Auth group threshold exceeded • Radius NAS threshold exceeded • Auth event rate threshold exceeded • Auth failure rate threshold exceeded • User lockout detected.

4. In *SNMP Hosts*, select *Add another SNMP Host* and enter the following information:

IP/Netmask	Enter the IP address and netmask of the host.
Queries	Select if this host uses queries.
Traps	Select if this host uses traps.
Delete	Select to delete the host.

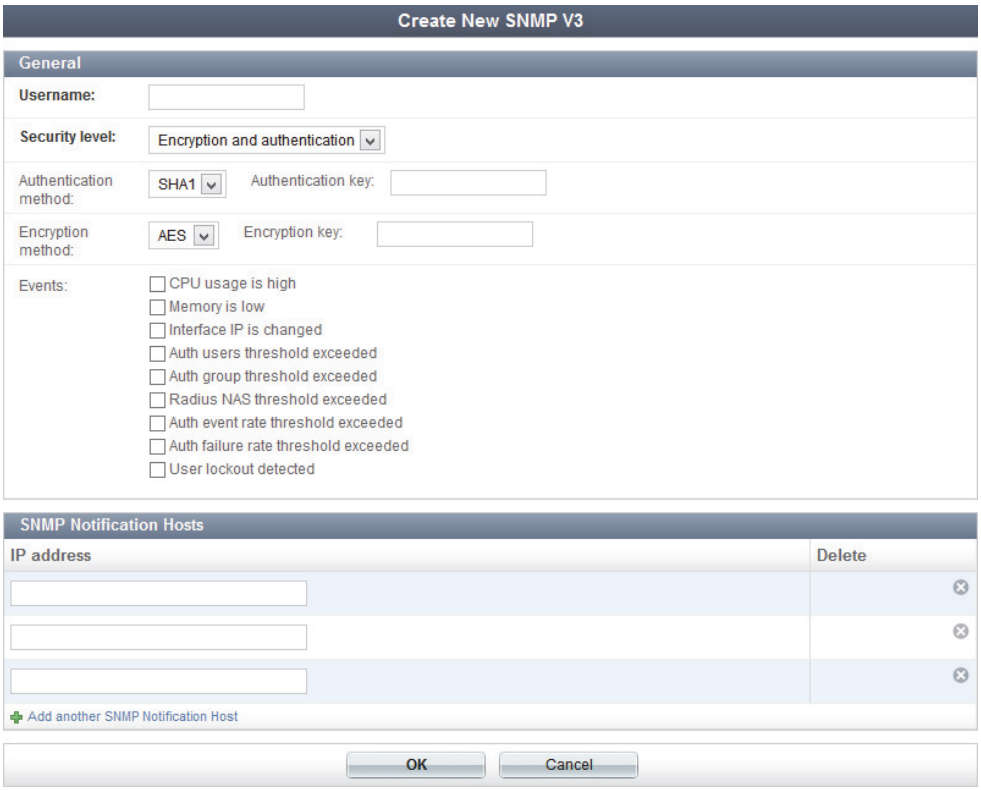
5. Select *OK* to create the new SNMP community.

To create a new SNMP user:

1. Go to *System* > *Administration* > *SNMP.*
2. Select *Create New* under *SNMP v3*.

   The *Create New SNMP V3* window opens.

Figure 33: New SNMP V3



3. Enter the following information in the *General* section:

Username	The name of the SNMP user.
Security Level	Select the security level from the drop-down list: • *None*: no authentication or encryption • *Authentication only*: select *Authentication method* then enter the authentication key in the *Authentication key* field • *Encryption and authentication*: select *Authentication method*, enter the authentication key in the *Authentication key* field, then select *Encryption method* and enter the encryption key in the *Encryption key* field.
Events	Select the events for which traps are enabled. See “Events” on page 52.

4. In *SNMP Notification Hosts*, select *Add another SNMP Notification Host* and enter the following information:

IP/Netmask	Enter the IP address and netmask of the notification host.
Delete	Select to delete the notification host.

5. Select *OK* to create the new SNMP V3 user.

Licensing

FortiAuthenticator-VM works in evaluation mode until it is licensed. In evaluation mode, only a limited number of users can be configured on the system. To expand this capability, a stackable licence can be applied to the system to increase both the user count, and all other metrics associated with the user count.

When a license is purchased, a registration code is provided. Go to support.fortinet.com and register your device by entering the registration code. You will be asked for the IP address of your FortiAuthenticator unit, and will then be provided with a license key.

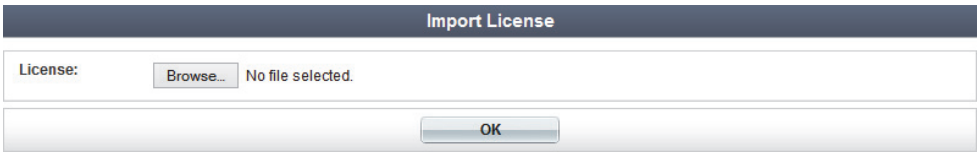
Ensure that the IP address specified while registering your unit is configured on one of the device's network interfaces, then upload the license key to your FortiAuthenticator-VM.

The *License Information* widget shows the current state of the device license. See "License Information widget" on page 40.

To license FortiAuthenticator:

1. Register your device.
2. Ensure that one of your device's network interfaces is configured to the IP address specified during registration.
3. Go to *System* > *Administration* > *Licensing*.

Figure 34: Import license file

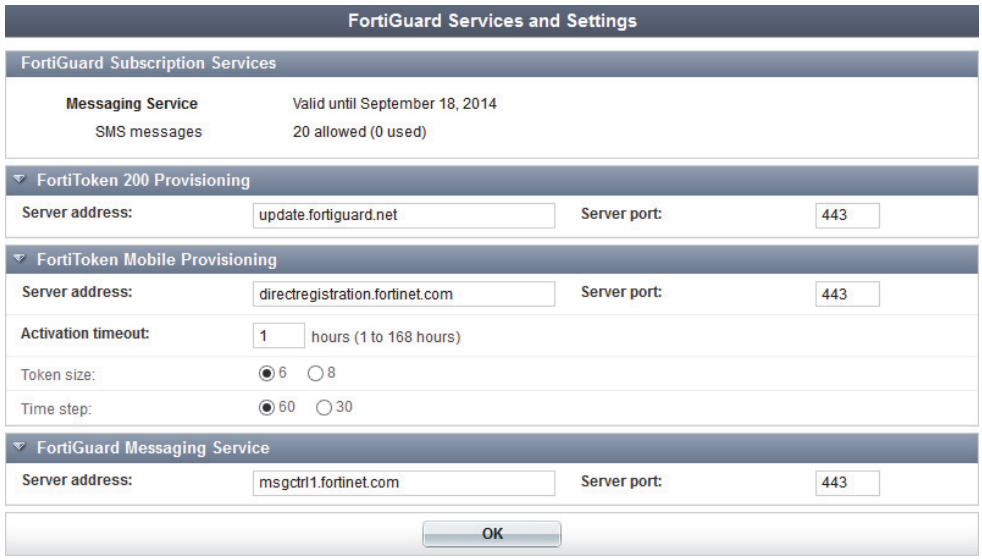


4. Select *Browse...* and locate, on your local computer, the license file you received from Fortinet.
5. Select *OK*.

FortiGuard

To view and configure FortiGuard connections, go to *System* > *Administration* > *FortiGuard*. The FortiGuard Distribution Network (FDN) page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see the FortiGuard Center web page.

Figure 35: FortiGuard services and settings



Configure the following settings, then select *OK* to apply them:

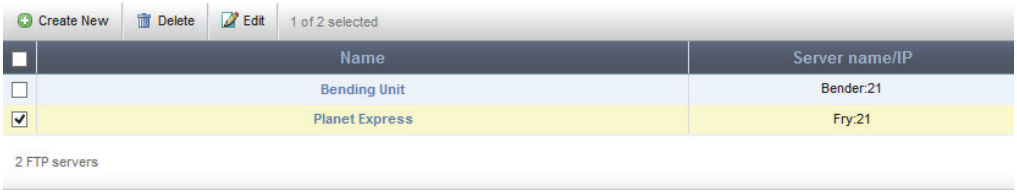
FortiGuard Subscription Services	
Messaging Service	The data to which the messaging service license is valid.
SMS messages	The total number of allowed SMS messages, and the number of messages that have been used.
FortiToken 200 Provisioning	
Server address	The server address.
Server port	The server port.
FortiToken Mobile Provisioning	
Server address	The server address.
Server port	The server port.
Activation timeout	The activation timeout in hours, from 1 to 168 hours.
Token size	The token size, either 6 or 8.
Time step	The time step, either 60 or 30.

FortiGuard Messaging Service	
Server address	The server address.
Server port	The server port.

FTP Servers

To view a list of the configured FTP servers, go to *System* > *Administration* > *FTP Servers*.

Figure 36:FTP servers



The following information is shown:

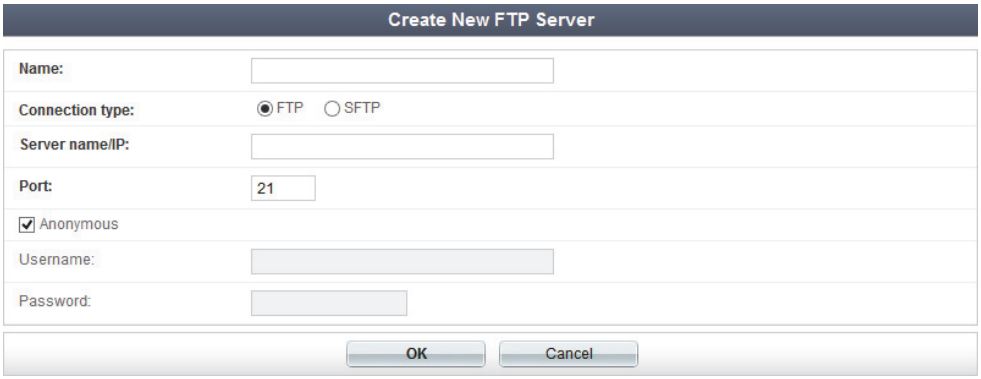
Create New	Select to create a new FTP server. See "To create a new FTP server:" on page 56.
Delete	Select to delete the selected FTP server or servers.
Edit	Select to edit the selected FTP server.
Name	The name of the FTP server.
Server name/IP	The server name or IP address, and port number.

To create a new FTP server:

1. Select *Create New*.

   The *Create New FTP Server* window will open.

   Figure 37: New FTP server



2. Enter the following information:

Name	Enter a name for the FTP server.
Connection type	Select the connection type, either *FTP* or *SFTP*.

Server name/IP	Enter the server name or IP address.
Port	Enter the port number.
Anonymous	Select to make the server anonymous.
Username	Enter the server username (if *Anonymous* is unselected).
Password	Enter the server password (if *Anonymous* is unselected).

3. Select *OK* to create the new FTP server.

Messaging

The FortiAuthenticator unit sends email for several purposes, such as password reset requests, new user approvals, user self-registration, and two-factor authentication.

By default, the FortiAuthenticator unit uses its built-in Simple Mail Transfer Protocol (SMTP) server. This is provided for convenience, but is not necessarily optimal for production environments. Fortinet recommends that you configure the unit to use a reliable external mail relay.

There are two distinct email services:

- Administrators - password reset, new user approval, two-factor authentication, etc.
- Users - password reset, self-registration, two-factor authentication, etc.

If you will send SMS messages to users, you must configure the SMS gateways that you will use. Ask your SMS provider for information about using its gateway. The FortiAuthenticator SMS gateway configuration differs according to the protocol your SMS provider uses.

SMTP Servers

To view a list of the SMTP servers, go to *System* > *Messages* > *SMTP Servers*.

Figure 38:SMTP servers

The following information is shown:

Create New	Select to create a new SMTP server. See "To add an external SMTP server:" on page 58.
Delete	Select to delete the selected SMTP server or servers.
Edit	Select to edit the selected SMTP server.
Set as Default	Set the selected SMTP server as the default SMTP server.
Name	The name of the SMTP server.

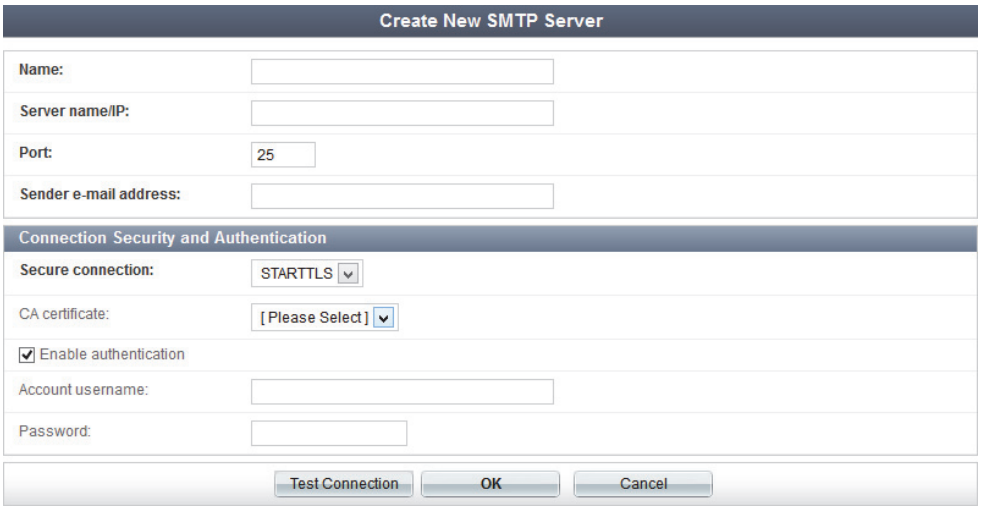
Server	The server name and port number.
Default	Shows a green circle with a check mark for the default SMTP server. To change the default server, select the server you would like to use as the default, then select *Set as Default* in the toolbar.

To add an external SMTP server:

1. Go to *System* > *Messages* > *SMTP Servers* and select *Create New*.

   The *Create New SMTP Server* window opens.

   Figure 39: New SMTP server



2. Enter the following information:

Name	Enter a name to identify this mail server on the FortiAuthenticator unit.
Server Name/IP	Enter the IP address or FQDN of the mail server.
Port	The default port 25. Change it if your SMTP server uses a different port.
Sender e-mail address	Enter the email address to put in the From field on email messages from the FortiAuthenticator unit.
Secure connection	For a secure connection to the mail server, select STARTTLS and select the CA certificate that validates the server's certificate. For information about importing the CA certificate, see "To import a CA certificate" on page 88.
Enable authentication	Select if the email server requires you to authenticate when sending email. Enter the *Account username* and *Password* if required.

3. Optionally, select *Test Connection* to send a test email message. Specify a recipient and select *Send*. Confirm that the recipient received the message.

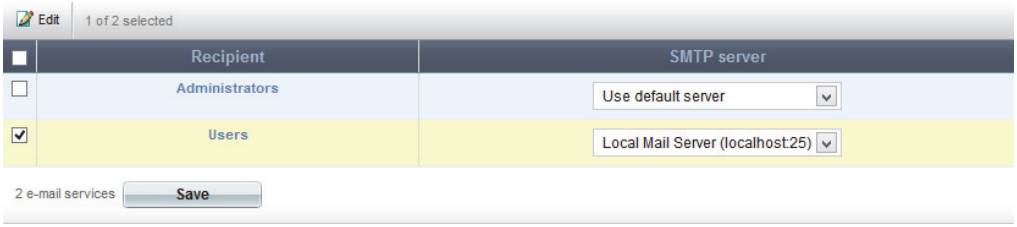
The recipient's email system might treat the test email message as spam.

4. Select *OK* to create the new SMTP server.

E-mail Services

To view a list of the email services, go to *System* > *Messages* > *E-mail Services*.

Figure 40: Email services



The following information is shown:

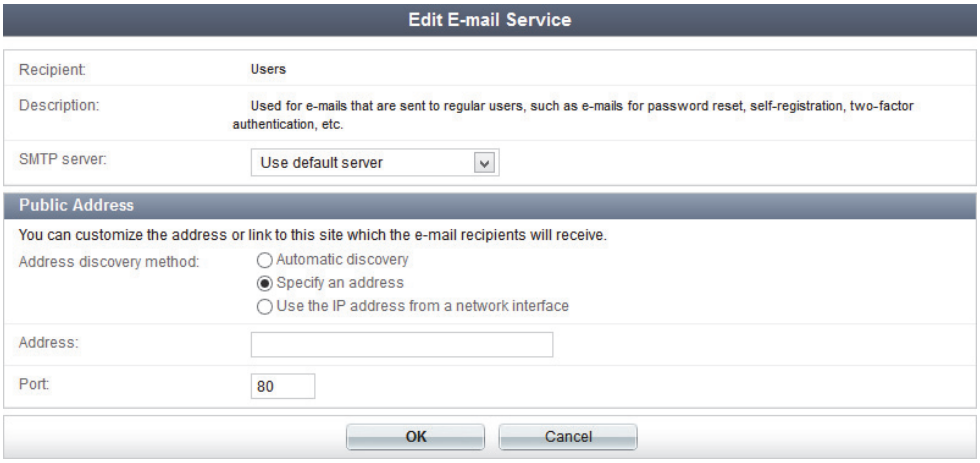
Edit	Select to edit the selected email service. See "To configure email services:" on page 60.
Recipient	The name of the email recipient.
SMTP server	The SMTP server associated with the recipient. The server can be selected from the drop-down list.
Save	Select to save any changes made to the email services.

To configure email services:

1. Go to *System* > *Messages* > *E-mail Services* and select the recipient you are editing.

   The *Edit E-mail Service* window opens.

Figure 41: Edit email service



2. Configure the following:

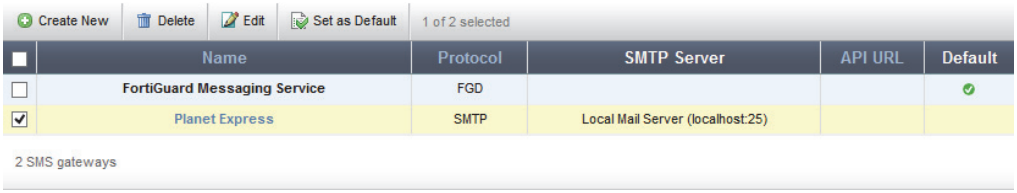
SMTP Server	Select the SMTP server from the drop-down list.
Public Address	Customize the address or link for the email.
Address discovery method	Select the address discover method: • *Automatic Discovery*: Use DNS domain name if configured, or automatically obtain address from the browser or an active network interface. • *Specify an address*: Manually enter the address and port number. • *Use the IP address from a network interface*: Select a specific network interface from the drop-down list.
Address	Enter the recipient address. Only available in *Address discovery method* is set to *Specify an Address*.
Port	Enter the recipient port number. Only available in *Address discovery method* is set to *Specify an Address*.
Network interface	Select a network interface from the drop-down list. Only available in *Address discovery method* is set to *Use the IP address from a network interface*.

3. Select *OK* to apply your changes.

SMS Gateways

To view a list of the configured SMS gateways, go to *System* > *Messages* > *SMS Gateways*.

Figure 42:SMS gateways



The following information is shown:

Create New	Select to create a new SMS gateway. See "To create a new SMTP SMS gateway:" on page 62 and "To create a new HTTP or HTTPS SMS gateway:" on page 63.
Delete	Select to delete the selected SMS gateway or gateways.
Edit	Select to edit the selected SMS gateway.
Set as Default	Set the selected SMS gateway as the default SMS gateway.
Name	The name of the SMS gateway.
Protocol	The protocol used by the gateway.
SMTP server	The SMTP server associated with the gateway.
API URL	The gateway's API URL, if it has one.
Default	Shows a green circle with a check mark for the default SMS gateway. To change the default gateway, select the gateway you would like to use as the default, then select *Set as Default* in the toolbar.

You can also configure the message that you will send to users. You can use the following tags for user-specific information:

Table 6: Tags used in SMS messages

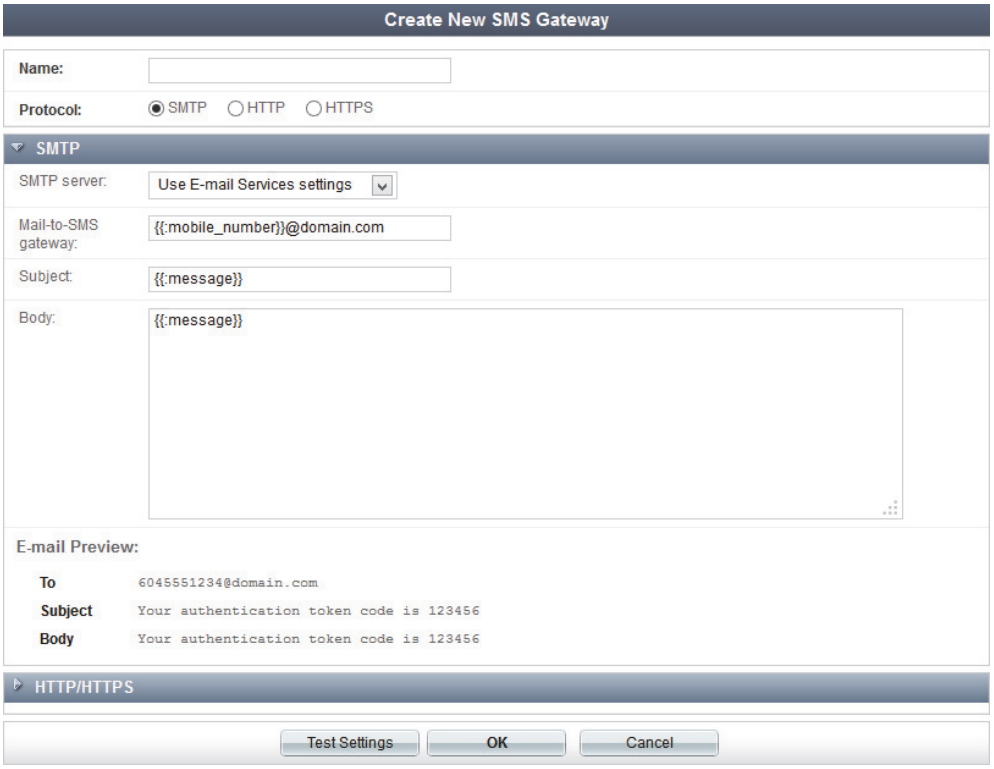
Tag	Information
{{:country_code}}	Telephone country code, e.g.: 01 for North America.
{{:mobile_number}}	User's mobile phone number
{{:message}}	"Your authentication token code is " and the code.

To create a new SMTP SMS gateway:

1. Go to *System* > *Messages* > *SMS Gateways* and select *Create New*.

   The *Create New SMS Gateway* window opens.

Figure 43: New SMTP SMS gateway



2. Enter the following information:

Name	Enter a name for the new gateway.
Protocol	Select SMTP.
SMTP server	Select the SMTP server you use to contact the SMS gateway. The SMTP server must already be configured, see "SMTP Servers" on page 57.
Mail-to-SMS gateway	Change `domain.com` to the SMS provider's domain name. The default entry `{{:mobile_number}}@domain.com` assumes that the address is the user's mobile number followed by @ and the domain name. In the *E-mail Preview* field, check the *To* field to ensure that the format of the address matches the information from your provider.
Subject	Optionally, enter a subject for the message.
Body	Optionally, enter body text for the message.
E-mail Preview	View a preview of the email message.

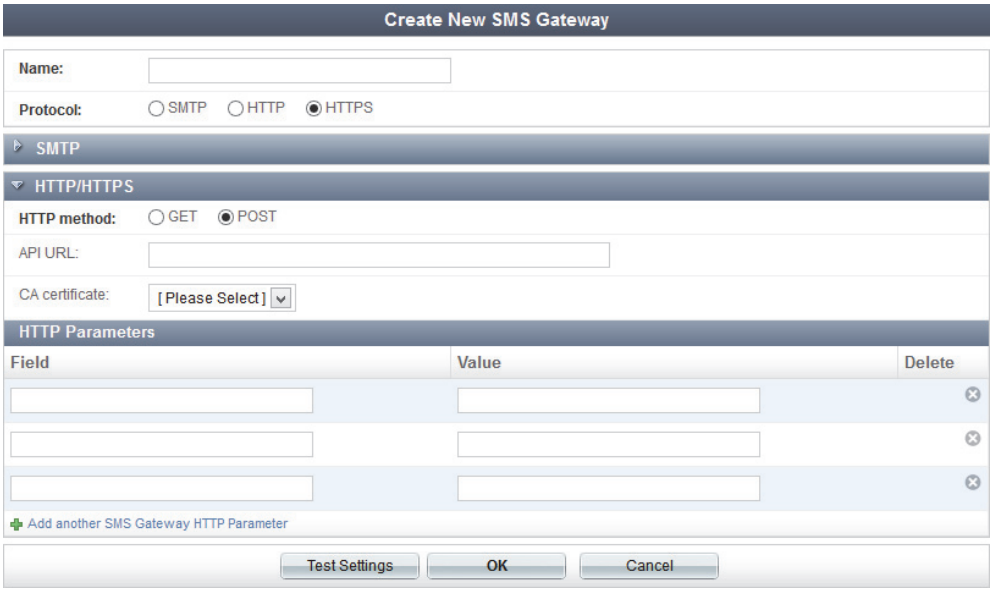
3. Optionally, select *Test Settings* to send a test SMS message to the user.
4. Select *OK* to a new SMTP SMS gateway.

To create a new HTTP or HTTPS SMS gateway:

1. Go to *System* > *Messages* > *SMS Gateways* and select *Create New*.

   The *Create New SMS Gateway* window opens.

   Figure 44: New HTTP or HTTPS SMS gateway



2. Enter the following information:

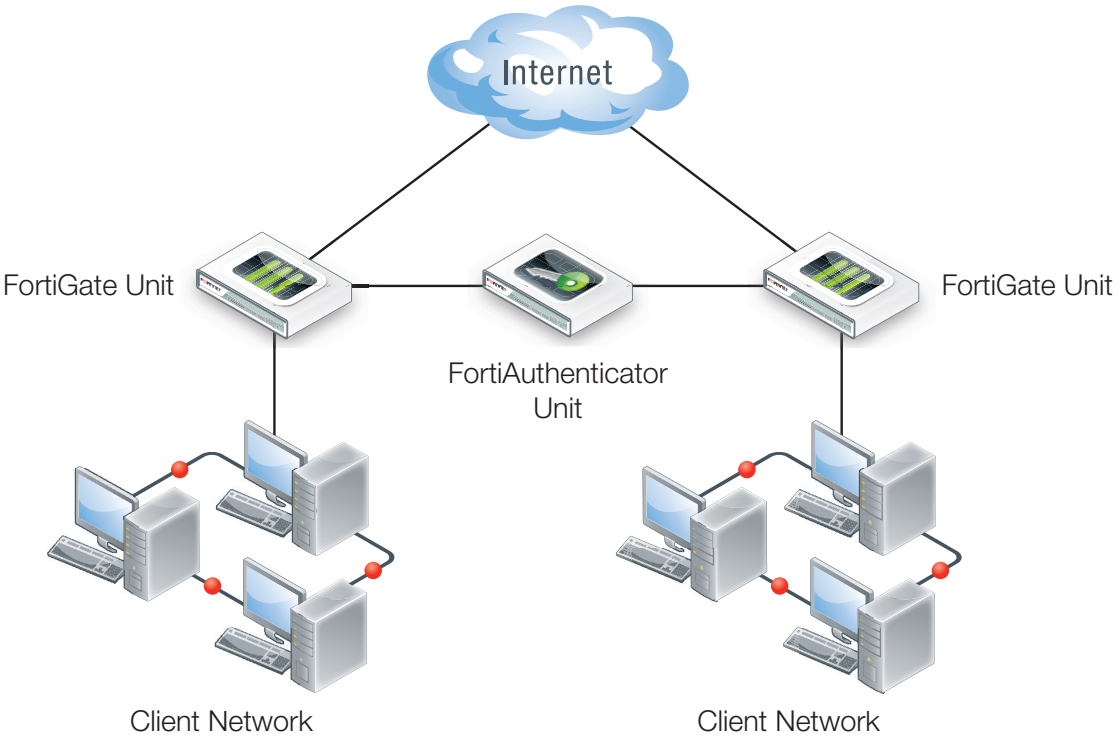
Name	Enter a name for the new gateway.
Protocol	Select HTTP or HTTPS.
HTTP/HTTPS	
HTTP method	Select the method to use, either *GET* of *POST*.
API URL	Enter the gateway URL, omitting the protocol prefix `http://` or `https://`. Also omit the parameter string that begins with `?`.
CA certificate	Select CA certificate that validates this SMS provider from the drop-down list. This option is only available if *Protocol* is set to *HTTPS*.
HTTP Parameters	
Field	Enter the parameter names that the SMS provider's URL requires, such as `user` and `password`.
Value	Enter the values or tags corresponding to the fields.
Delete	Delete the field and its value.

3. If you need more parameter entries, select *Add another SMS Gateway HTTP Parameter.*
4. Optionally, select *Test Settings* to send a test SMS message to the user.
5. Select *OK* to a new HTTP or HTTPS SMS gateway.

Authentication

FortiAuthenticator provides an easy to configure authentication server for your users. Multiple FortiGate units can use a single FortiAuthenticator unit for remote authentication and FortiToken device management.

Figure 45: FortiAuthenticator in a multiple FortiGate unit network



This chapter includes the following topics:

What to configure

You need to decide which elements of FortiAuthenticator configuration you need.

- Determine the type of authentication you will use: password-based or token-based. Optionally, you can enable both types, this is called two-factor authentication.
- Determine the type of authentication server you will use: RADIUS, built-in LDAP, or Remote LDAP. You will need to use at least one of these server types.
- Determine which FortiGate units or third-party devices will use the FortiAuthenticator unit. The FortiAuthenticator unit must be configured on each FortiGate unit as an authentication server, either RADIUS or LDAP. For RADIUS authentication, each FortiGate unit or third-party device must be configured on the FortiAuthenticator unit as an authentication client.

Password-based authentication

User accounts can be created on the FortiAuthenticator device in multiple ways:

- Administrator creates a user and specifies their username and password.
- Administrator creates a username and a random password is automatically emailed to the user.
- Users are created by importing a CSV file.

Users can self-register for password-based authentication. This reduces the workload for the system administrator. Users can choose their own passwords or have a randomly generated password provided in the browser or sent to them through email or SMS. Self-registration can be instant, or it can require administrator approval. See "Self-registration" on page 91.

Once created, users are automatically part of the RADIUS Authentication system and can be authenticated remotely.

See "User management" on page 70 for more information about user accounts.

Two-factor authentication

Two-factor authentication increases security by requiring multiple pieces of information on top of the username and password. There are generally two factors:

- something the user knows, usually a password,
- something the user has, such as a FortiToken device.

Requiring the two factors increases the difficulty for an unauthorized person to impersonate a legitimate user.

To enable two-factor authentication, configure both password-based and token-based authentication in the user's account.

FortiAuthenticator token-based authentication requires the user to enter a numeric token at login. Two types of numerical tokens are supported:

- Time based: TOTP (RFC 6238)

  The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.

  Passcodes can only be used a single time (one time passcodes) to prevent replay attacks. Fortinet has the following time based tokens:

  - FortiToken 200
  - FortiToken Mobile, running on a compatible smartphone
- Event based: HMAC-based One Time Password (HTOP) (RFC 4226)

  The token passcode is generated using an event trigger and a secret key. Event tokens are supported using a valid email account and a mobile phone number with SMS service.

  FortiToken devices, FortiToken Mobile apps, email addresses, and phone numbers must be configured in the user's account.

  Only the administrator can configure token-based authentication. See "Configuring token based authentication" on page 75.

Authentication servers

The FortiAuthenticator unit has built-in RADIUS and LDAP servers. It also supports the use of remote LDAP, which can include Windows AD servers.

The built-in servers are best used where there is no existing authentication infrastructure. You build a user account database on the FortiAuthenticator unit. The database can include additional user information such as street addresses and phone numbers that cannot be stored in a FortiGate unit's user authentication database. You can use either LDAP or RADIUS protocols. The remote LDAP option adds your FortiGate units to an existing LDAP structure. Optionally, you can add two-factor authentication to remote LDAP.

RADIUS

If you use RADIUS, you must enable RADIUS in each user account. FortiGate units must be registered as a RADIUS authentication clients in *Authentication* > *RADIUS Service* > *Clients*. See "Adding a RADIUS authentication client" on page 97. On each FortiGate unit that will use the RADIUS protocol, the FortiAuthenticator unit must be configured as a RADIUS server in *User & Device* > *Authentication* > *RADIUS Server*.

Built-in LDAP

If you use built-in LDAP, you will need to configure the LDAP directory tree. You add users from the user database to the appropriate nodes in the LDAP hierarchy. See "Creating the directory tree" on page 101. On each FortiGate unit that will use LDAP protocol, the FortiAuthenticator unit must be configured as an LDAP server in *User & Device* > *Authentication* > *LDAP Server*.

Remote LDAP

Remote LDAP is used when an existing LDAP directory exists and should be used for authentication. User information can be selectively synchronised with the FortiAuthenticator unit, but the user credentials (passwords) remain on, and are validated against the LDAP directory.

To utilize remote LDAP, the authentication client (such as a FortiGate device) must connect to the FortiAuthenticator device using RADIUS to authenticate the user information (see *User & Device* > *Authentication* > *RADIUS Server*). The password is then proxied to the LDAP server for validation, while any associated token passcode is validated locally.

User account policies

General policies for user accounts include lockout settings, password policies, and custom user fields.

Lockouts

For various security reasons, you may want to lock a user's account. For example, repeated unsuccessful attempts to log in might indicate an attempt at unauthorized access.

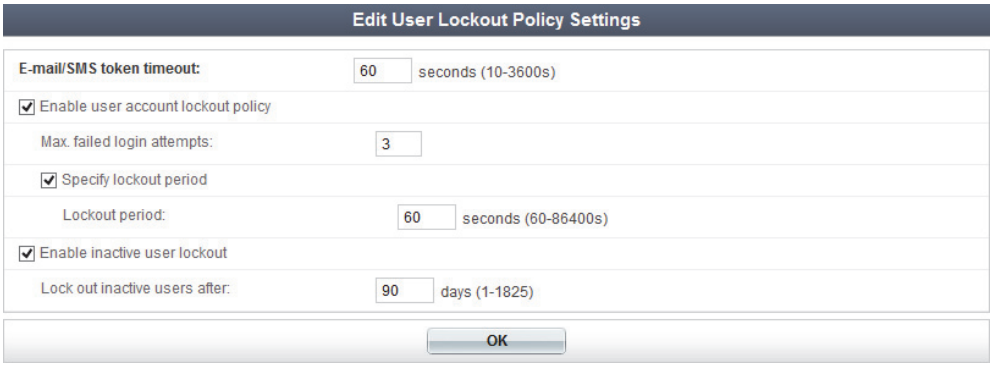
Information on locked out users can be viewed in the *Top User Lockouts* widget, see "Top User Lockouts widget" on page 41.

Currently locked out users can be viewed in *Monitor* > *Authentication* > *Inactive Users*, see "Inactive users" on page 134.

To configure the user lockout policy:

1. Go to *Authentication* > *User Account Policies* > *Lockouts*.

Figure 46: User lockout configuration



2. Configure the following settings:

E-mail/SMS token timeout	Set a time after which a token code sent via email or SMS will be marked as expired, from 10 to 3600 seconds.
Enable user account lockout policy	Enable user account lockout for failed login attempts and enter the maximum number of allowed failed attempts in the *Max. failed login attempts* field.

Specify lockout period	Select to specify the length of the lockout period, from 60 to 86400 seconds. After the lockout period expires, the *Max. failed login attempts* number applies again. When disabled, locked out users will be permanently disabled until an administrator manually re-enables them.
Enable inactive user lockout	Select to enable disabling a user account if there is no login activity for a given number of days. In the *Lock out inactive users after* field, enter the number of days, from 1 to 1825, after which a user is locked out.

3. Select OK to apply the account lockout settings.

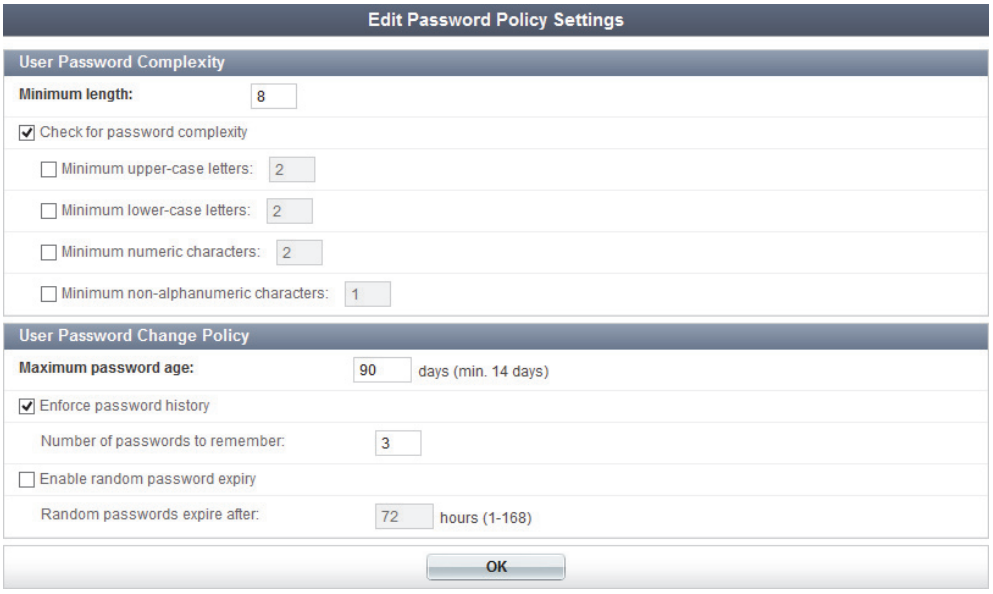
Passwords

You can enforce a minimum length and complexity for user passwords, and can force users to change their passwords periodically.

For information on setting a user's password, and password recovery options, see "Editing a user" on page 73.

Go to *Authentication* > *User Account Policies* > *Passwords* to configure password policy settings.

Figure 47: Password policy configuration



To set password complexity requirements:

1. In *User Password Complexity*, enter the minimum password length in the *Minimum length* field.

   The default minimum length is 0, which means that there is no minimum length but the password cannot be empty.

2. Optionally, select *Check for password complexity*. and then configure the following password requirements as needed:
   - Minimum upper-case letters
   - Minimum lower-case letters
   - Minimum numeric characters
   - Minimum non-alphanumeric characters
3. Select *OK* to apply the password length and complexity settings.

To set a password change policy:

1. In *User Password Change Policy*, set the maximum allowed password age in the *Maximum password age* field.

   The default maximum password age is 90 days. The minimum value allowed is 14 days.
2. Optionally, select *Enforce password history* to prevent users from creating a new password that is the same as their current password or recently used passwords.

   Then, enter the number of password to remember in the *Number of passwords to remember* field. New passwords must not match any of the remembered passwords. For example, if three passwords are remembered, users cannot reuse any of their three previous passwords.
3. Optionally, select *Enable random password expiry* to force randomly generated passwords to expire. Then, enter the length of time after which a randomly generated password will expire in the *Random passwords expire after* field.

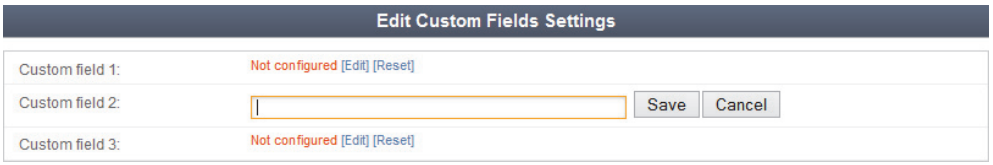
   The default randomly generated password expiry age is 72 hours. The value can be set from 1 to168 hours.
4. Select *OK* to apply the password change policy settings.

Custom user fields

Custom fields can be created to be included in the user information of local users. See “Local users” on page 71 for information about creating and managing local users.

To edit custom fields, go to *Authentication* > *User Account Policies* > *Custom User Fields*.

Figure 48: Custom user fields



A maximum of three custom fields can be added.

User management

FortiAuthenticator's user database has the benefit of being able to associate extensive information with each user, as you would expect of RADIUS and LDAP servers. This information includes: whether the user is an administrator, uses RADIUS authentication, uses two-factor authentication, and personal information such as full name, address, password recovery options, and the groups that the user belongs to.

The RADIUS server on the FortiAuthenticator unit is configured using default settings. For a user to authenticate using RADIUS, the option *Allow RADIUS Authentication* must be selected for that user's entry, and the FortiGate unit must be added to the authentication client list. See "Adding a RADIUS authentication client" on page 97.

This section includes the following subsections:

Administrators

Administrator accounts on FortiAuthenticator are standard user accounts that are flagged as administrators. Both local users and remote LDAP users can be administrators.

Once flagged as an administrator, a user account's administrator privileges can be set to either full access or customized to select their administrator rights for different parts of the FortiAuthenticator unit. There are log events for administrator configuration activities. Administrators can also be configured to authenticate to the local system using two-factor authentication. An account marked as an administrator cannot be used for RADIUS authentication.

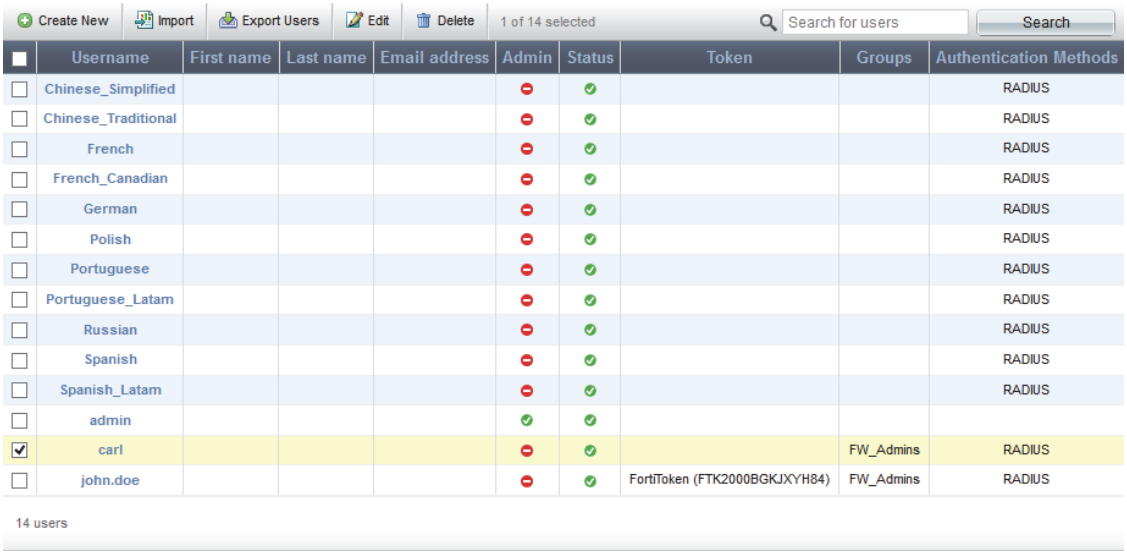
See "Configuring a user as an administrator" on page 76 for more information.

Local users

Local user accounts can be created, imported, exported, edited, and deleted as needed.

To manage local user accounts, go to *Authentication* > *User Management* > *Local Users*.

Figure 49: Local users list



The local user account list shows the following information:

Create New	Select to create a new user. See "Adding a user" on page 72.
Import	Select to import local user accounts from a CSV file or FortiGate configuration file. If using a CSV file, it must have one record per line, with the following format: user name (30 characters max), first name (30 characters max), last name (30 characters max), email address (75 characters max), mobile number (25 characters max), password (optional, 128 characters max). If the optional password is left out of the import file, the user will be emailed temporary login credentials and requested to configure a new password.
Export Users	Select to export the user account list to a CSV file.
Edit	Select to edit the selected user account. See "Editing a user" on page 73.
Delete	Select to delete the selected user account or accounts.
Search	Enter a search term in the search field, then select *Search* to search the user account list.
Username	The user accounts' usernames.
First name	The user accounts' first names, if included.
Last name	The user accounts' last names, if included.

Email address	The user accounts' email addresses, if included.
Admin	If the user account is set as an administrator, a green circle with a check mark is shown.
Status	If the user account is enabled, a green circle with a check mark is shown.
Token	The token that is assigned to that user account.
Groups	The group or groups to which the user account belongs.
Authentication Method	The authentication method used for the user account.

Adding a user

When creating a user account, there are three ways to handle the password:

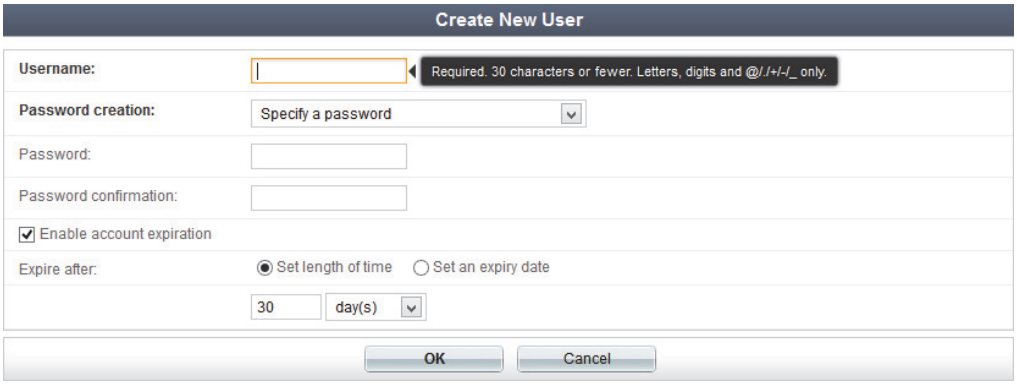
- The administrator assigns a password immediately and communicates it to the user.
- The FortiAuthenticator unit creates a random password and automatically emails it to the new user.
- No password is assigned because only token-based authentication will be used.

To add a new user:

1. In the local users list, select *Create New*.

   The *Create New User* window opens.

   Figure 50: Create a new user



2. Enter the following information:

Username	Enter a username for the user.
Password creation	Select one of three options from the drop-down list: • *Specify a password*: Manually enter a password in the *Password* field, then reenter the password in the *Password confirmation* field. • *Set and e-mail a random password*: Enter an email address to which to send the password in the *E-mail address* field, then reenter the email address in the *Confirm e-mail address* field. • *No password, FortiToken authentication only*: After you select *OK*, you will need to associate a FortiToken device with this user.
Enable account expiration	Select to enable account expiration, either after a specific amount of time has elapsed, or on a specific date.
Expire after	Select when the account will expire, one of: • *Set length of time*: Enter the amount of time in hours, days, months, or years, until the account expires. • *Set an expire date*: Enter the date on which the account will expire, either by manually typing it in, or by selecting the calendar icon then selecting a date on the pop-up calendar.

3. Select *OK* to create the new user.

   You will be redirected to the *Change user* window to continue the user configuration. See "Editing a user" on page 73.

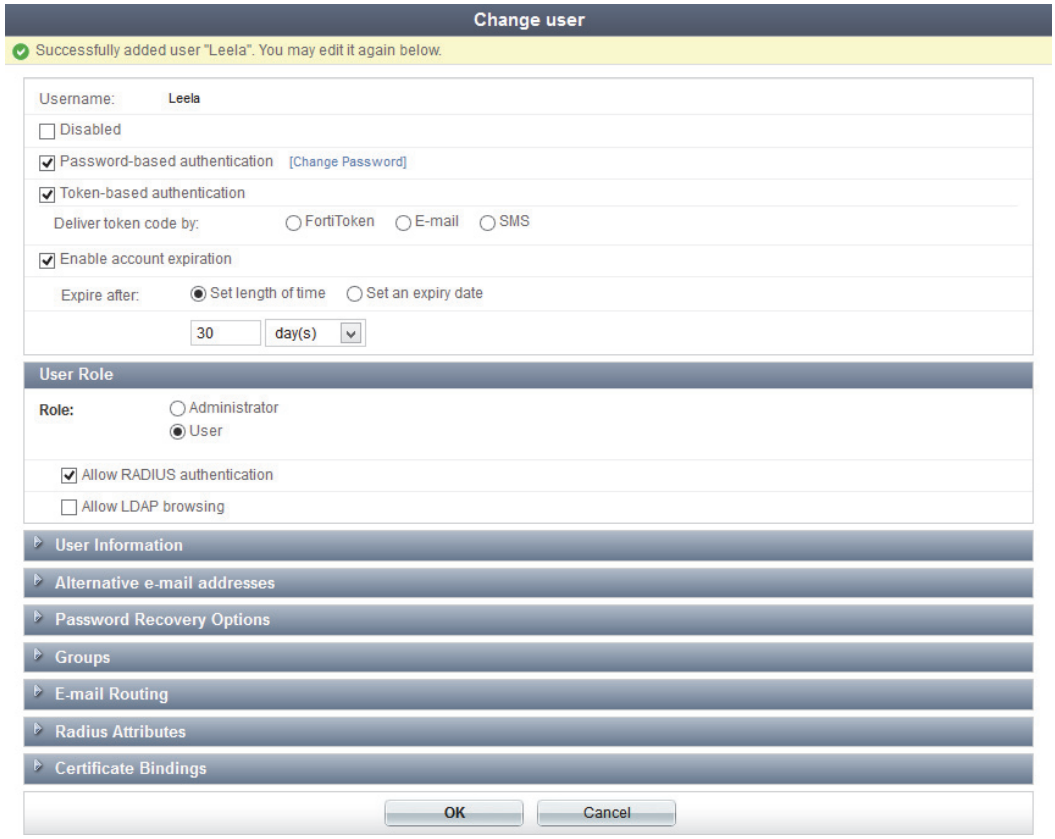
   If the password creation method was set to *No password, FortiToken authentication only* you will be required to associate a FortiToken with the user before the user can be enabled. See "Configuring token based authentication" on page 75.

Editing a user

User accounts can be edited at any time. When creating a new user, you will be immediately redirected to the *Change user* window to complete the user configuration.

To view the *Change user* window, go to the user account list, select the user you will be editing, and then select *Edit* from the toolbar. Conversely, selecting the username in the user list will also open the *Change user* window, see Figure 51 on page 74.

Figure 51: Change a user



The following information can be viewed or configured:

Username	The user's username. This cannot be changed.
Disabled	Select to disable the user account.
Password-based authentication	Select to enable password based authentication. Select *Change Password* to open the Change password window, where you can change the user's password.
Token-based authentication	Select to enable FortiToken based authentication. See "Configuring token based authentication" on page 75.
Enable account expiration	Select to enable account expiration. See "Enable account expiration" on page 73.
User Role	Configure the user's role.
Role	Select *Administrator* or *User*. If setting a user as an administrator, see "Configuring a user as an administrator" on page 76.
Allow RADIUS authentication	Select to allow RADIUS authentication. This applies only to non-administrator users.
Allow LDAP browsing	Select to Allow LDAP browsing.

User Information	Enter user information, such as their address and phone number. See “Adding user information” on page 76.
Alternative e-mail addresses	Add alternate email addresses for the user.
Password Recovery Options	Configure password recovery options for the user. See “Configuring password recovery options” on page 77
Groups	Assign the user to one or more groups. See “User groups” on page 83.
E-mail Routing	Enter a mail host and routing address into their respective fields to configure email routing for the user.
Radius Attributes	Add RADIUS attributes. See “RADIUS attributes” on page 85.
Certificate Bindings	Add certificate bindings to the user account. See “Configuring certificate bindings” on page 78.

Select *OK* when you have finished editing the user’s information and settings.

Configuring token based authentication

Token-based authentication requires one of the following:

- a FortiToken device or mobile device with the FortiToken Mobile app installed,
- a device with either email or SMS capability.

If a FortiToken device or FortiToken Mobile app will be used, it must first be registered in *Authentication* > *User Management* > *FortiTokens*. See “FortiTokens” on page 84 for more information.

To configure an account for token-based authentication:

1. Go to the *Change user* window for the requisite user account.
2. Select *Token-based authentication* to view the token-based authentication options.
3. Do one of the following:
   - Select *FortiToken*, then select the FortiToken device serial number from the *FortiToken 200* or *FortiToken Mobile* drop-down lists, as appropriate.

     The device must be known to the FortiAuthenticator unit. See “FortiToken devices and mobile apps” on page 86.

     Optionally, select *Configure a temporary e-mail/SMS token* to receive a temporary token code via email or SMS.
   - Select *Email* and enter the user’s email address in the *User Information* section.
   - Select *SMS* and enter the user’s mobile number in the *User Information* section.
4. Select *OK*.

By default, token-based authentication must be completed within 60 seconds after the token passcode is sent by email or SMS. To change this timeout, go to *Authentication* > *User Account Polices* > *Lockouts* and modify the *Email/SMS Token Timeout* field, see “Lockouts” on page 67.

Configuring a user as an administrator

See "Administrators" on page 70 for more information.

To set a user as an administrator:

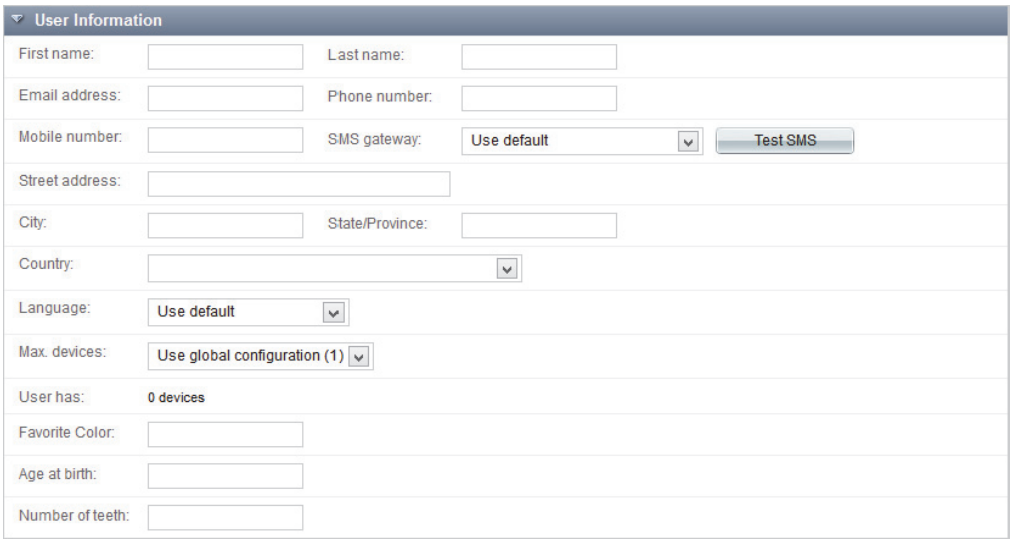
1. Go to the *Change user* window for the requisite user account.
2. In the User Role section, select *Administrator* for the *Role*.
3. In the *Access* field, select *Full* to give the administrator fill administrative privileges, or select *Custom* to customize the administrator's permissions.

   If *Custom* is selected, find the permissions that the user will have in the *Available user permissions* list, and move them to the *Selected user permissions* list.
4. Select *Web service access* to allow the administrator to access the web services via a REST API or FortiAuthenticator Agent for Microsoft Windows.
5. Select *Allow LDAP browsing* to allow the user to browse LDAP.
6. Select *OK* to apply the changes to the user.

Adding user information

User information can be added in the *Change user* window. Some information can be required depending on how the user is configured. For example, is the user is using token-based authentication by SMS, then a mobile number and SMS gateway must be configured before the user can be enabled.

Figure 52: User information



The following user information can be entered:

First name	*Last name*
Email address	*Phone number*
Mobile number	*SMS gateway*: select from the drop-down list. Select *Test SMS* to send a test message.
Street address	
City	*State/Province*
Country: Select from the drop-down list.	

Language: select a specific language from the drop-down list, or use the default language.
Max. devices: Select either *Use global configuration*, or *Specify a custom number*.
User has: The number of device the user currently has.
Custom user fields: See "Custom user fields" on page 69 for more information.

Configuring password recovery options

To replace a lost or forgotten password, the FortiAuthenticator unit can send the user a password recovery link by email or in a browser in response to a pre-arranged security question. The user then must set a new password.

To configure password recovery by email:

1. Go to the *Change user* window for the requisite user account.
2. Ensure that the user has an email address entered. See "Adding user information" on page 76.
3. In the *Password Recovery Options* section, Select *E-mail recovery*.
4. Optionally, select *Alternative e-mail addresses* and enter additional email addresses for this user.

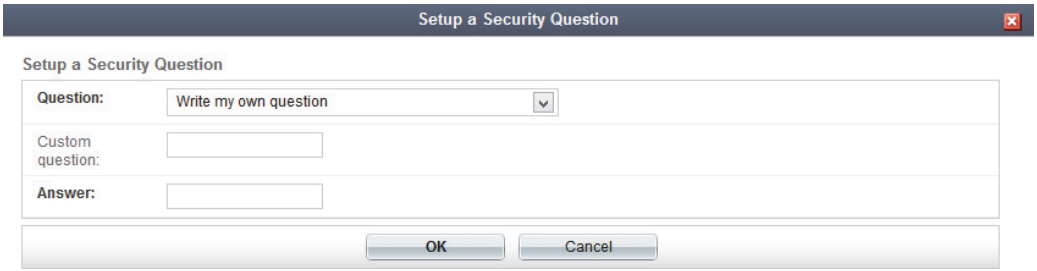
   In the event of password recovery, an email message will be sent to all configured email addresses — both the user information email address and the alternative email addresses.
5. Select *OK* to apply the changes.

To configure password recovery by security question:

1. Go to the *Change user* window for the requisite user account.
2. In the *Password Recovery Options* section, select *Security question*, then select *Edit*.

   The *Setup a Security Question* dialog box opens.

   Figure 53: Setup a security question



3. Choose one of the questions in the list, or select *Write my own question* and enter a question in the *Custom question* field.
4. Enter the answer for the question in the *Answer* field.
5. Select *OK* to create the security question.
6. Select *OK* in the *Change user* window to apply your changes.

How the user can configure password recovery by security question:

1. Log in to the user account. The *View Profile* page opens.
2. Select *Edit Profile* at the top left of the page.
3. In the *Password Recovery Options* section, select *Security Question*, and select *Edit*.

4. Choose one of the questions in the list, or select *Write my own question* and enter a question in the *Custom question* field.
5. Enter the answer for your question.
6. Select *OK*.

How the user can configure password recovery by email:

1. Log in to the user account. The *View Profile* page opens.
2. Select *Edit Profile* at the top left of the page.
3. In the *Password Recovery Options* section, select *E-mail recovery*.
4. Optionally, select *Alternative e-mail addresses* and enter additional email addresses for this user.
5. Select *OK*.

How the user recovers from a lost password:

1. Browse to the IP address of the FortiAuthenticator.

   Security policies must be in place on the FortiGate unit to allow these sessions to be established.
2. At the login screen, select *Forgot my password*.
3. Select either *Username* or *Email* as your method of recovery.
4. Enter either your username or email address as selected in the previous step, and then select *Next*.

   This information is used to select the user account. If your information does not match a user account, password recovery cannot be completed.
5. Do one of the following:
   - If an email address was entered, check your email, open the email and select the password recovery link.
   - If a username was entered, answer the security question and then select *Next*.

   The recovery options available depend on the settings in the user account.
6. On the *Reset Password* page, enter and confirm a new password and then select *Next*.

   The user can now authenticate using the new password.

Configuring certificate bindings

To use a local certificate as part of authenticating a user, you need to:

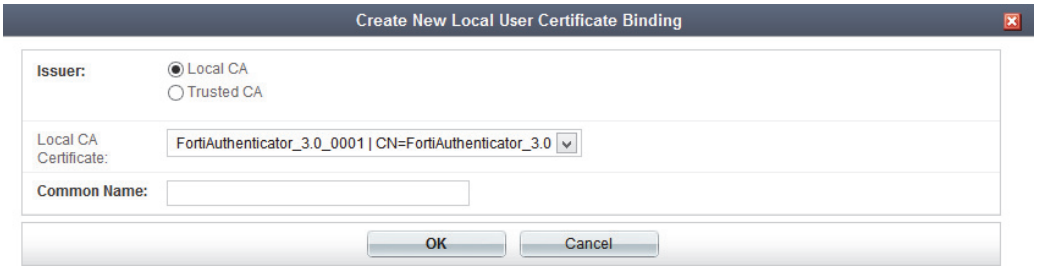
- Create a user certificate for the user, see "User and server certificates" on page 90.
- Create a binding to that certificate in the user's account.

To create a binding to a certificate in a user's account:

1. Go to the *Change user* window for the requisite user account.
2. In the *Certificate Bindings* section, select *Add Binding*.

   The *Create New Local User Certificate Binding* window opens.

Figure 54: New local user certificate binding



3. Select either *Local CA* or *Trusted CA* and then select the applicable CA certificate from the drop-down list.
4. Enter the *Common Name* on the certificate. For example, if the certificate says `CN=rgreen` then enter `rgreen`.
5. Select *OK* to add the new binding.

Remote users

Remote LDAP users must be imported into the FortiAuthenticator user database. Remote users can be imported from LDAP servers, see "Remote LDAP servers" on page 95.

A maximum of five users can be imported.

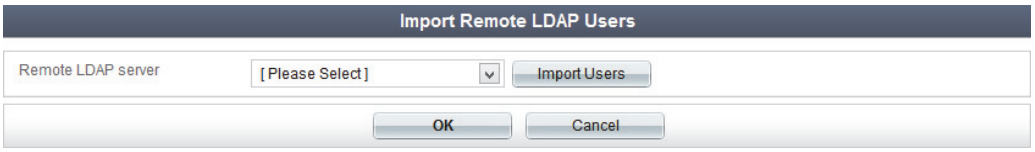
A FortiToken device already allocated to a local account cannot be allocated to an LDAP user as well; it must be a different FortiToken device.

To import remote LDAP users:

1. Go to *Authentication* > *User Management* > *Remote Users* and select *Import.*

   The *Import Remote LDAP Users* screen open.

   Figure 55: Import remote LDAP users

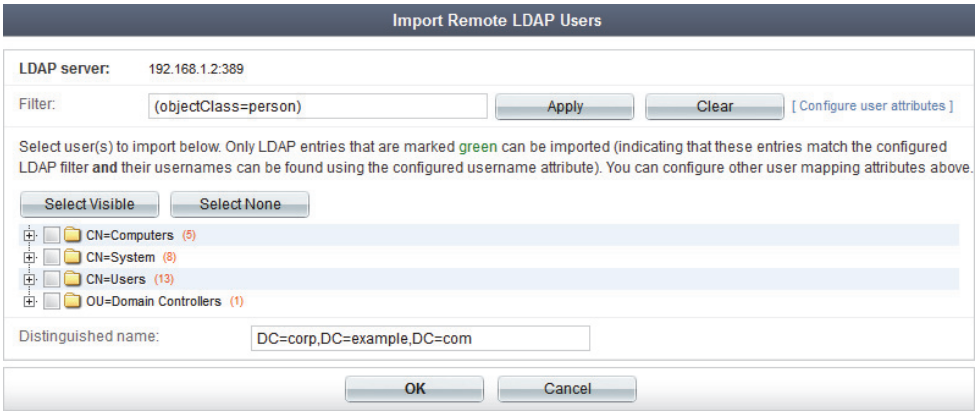


2. Select a remote LDAP server from the *Remote LDAP Server* drop-down list, then select *Import Users*.

An LDAP server must already be configured to select it in the drop-down list. See "Remote LDAP servers" on page 95 for information on adding a remote LDAP server.

The *Import Remote LDAP Users* window opens in a new browser window.

Figure 56: Import remote LDAP users



3. Optionally, enter a *Filter* string to reduce the number of entries returned, and then select *Apply*, or select *Clear* to clear the filters.

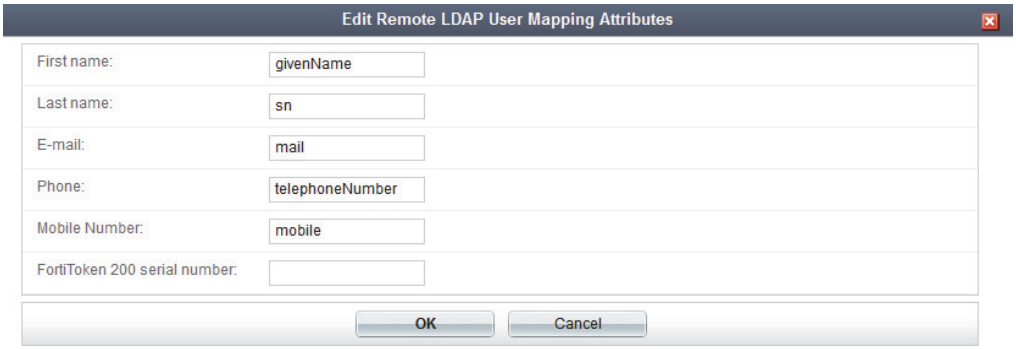
   For example, `uid=j*` returns only user IDs beginning with “j”.

4. Select the entries you want to import and then select *OK*.

   The amount of time required to import the remote users will vary depending on the number of users being imported.

The default configuration imports the attributes commonly associated with Microsoft Active Directory LDAP implementations. Select *Configure user attributes* to edit the remote LDAP user mapping attributes.

Figure 57: Edit remote LDAP user mapping attributes



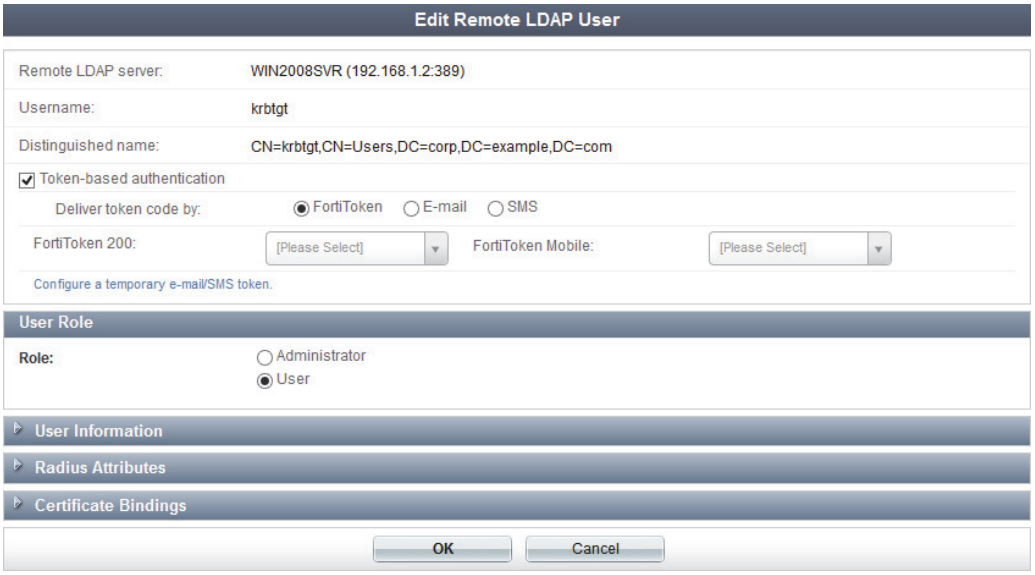
Selecting the field, *FirstName* for example, presents a list of attributes which have been detected and can be selected. This list is not exhaustive and additional, non-displayed attributes may be available for import. Consult your LDAP administrator for a list of available attributes.

To add two-factor authentication to a remote LDAP user:

1. From the remote user list, select the user you are editing.

   The *Edit Remote LDAP User* window opens.

Figure 58: Edit remote LDAP user



2. Select *Token-based authentication*, then follow the same steps as when editing a local user ("Editing a user" on page 73).
3. Configure the *User Role*, *User Information*, *Radius Attributes*, and *Certificate Bindings* for the user as needed.
4. Select *OK* to apply the changes.

Remote user sync rules

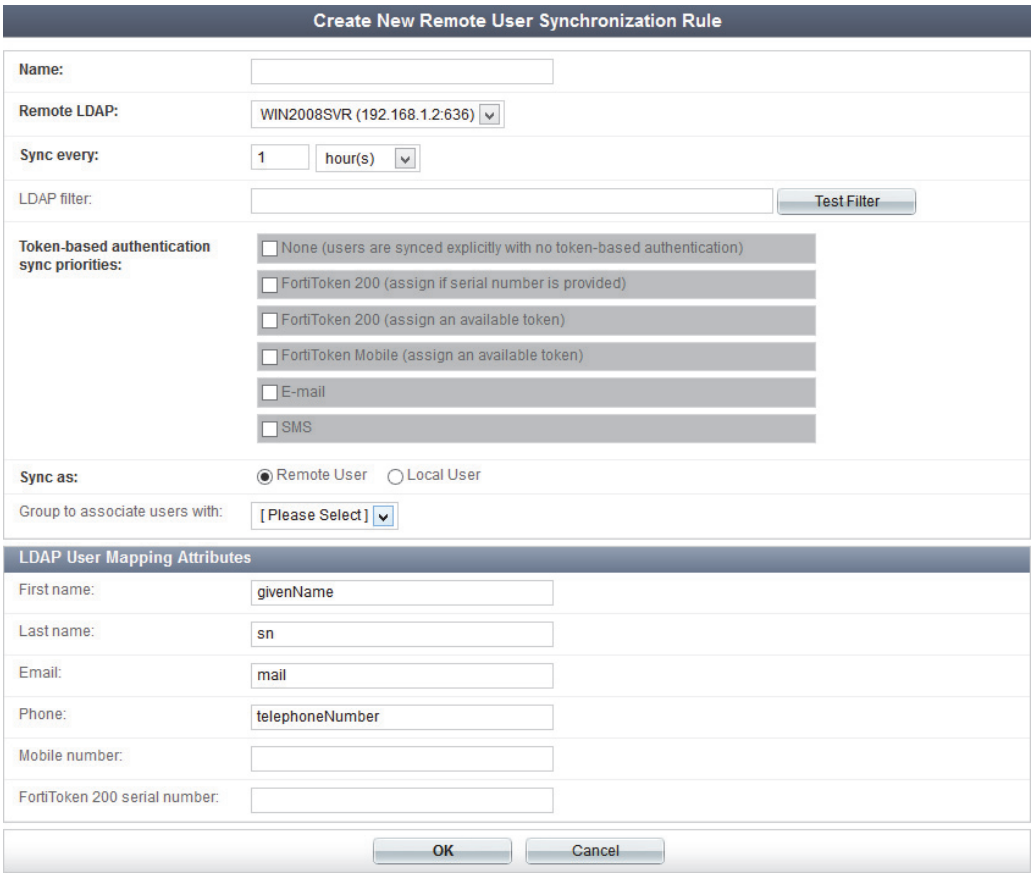
Synchronization rules can be created to control how and when remote users are synchronized. To view a list of the remote user synchronization rules, go to *Authentication* > *User Management* > *Remote User Sync Rules*.

To create a new remote user synchronization rule:

1. From the *Remote User Sync Rules* page, select *Create New*.

   The *Create New Remote User Synchronization Rule* windows opens.

Figure 59: New remote user synchronization rule



2. Configure the following settings:

Name	Enter a name for the synchronization rule.
Remote LDAP	Select a remote LDAP server from the drop-down list. To configure a remote LDAP server, see “Remote LDAP servers” on page 95.
Sync every	Select the amount of time between synchronizations.
LDAP filter	Optionally, enter an LDAP filter. Select *Test Filter* to test that the filter functions as expected.
Token-based authentication sync priorities	Select the required authentication synchronization priorities. Drag the priorities up and down in the list change the priority order.

Sync as	Select to synchronize as a remote user or as a local user.
Group to associate users with	Optionally, select a group from the drop-down list with which to associate the users with.
LDAP User Mapping Attributes	Optionally, edit the remote LDAP user mapping attributes.

3. Select *OK* to create the new synchronization rule.

User groups

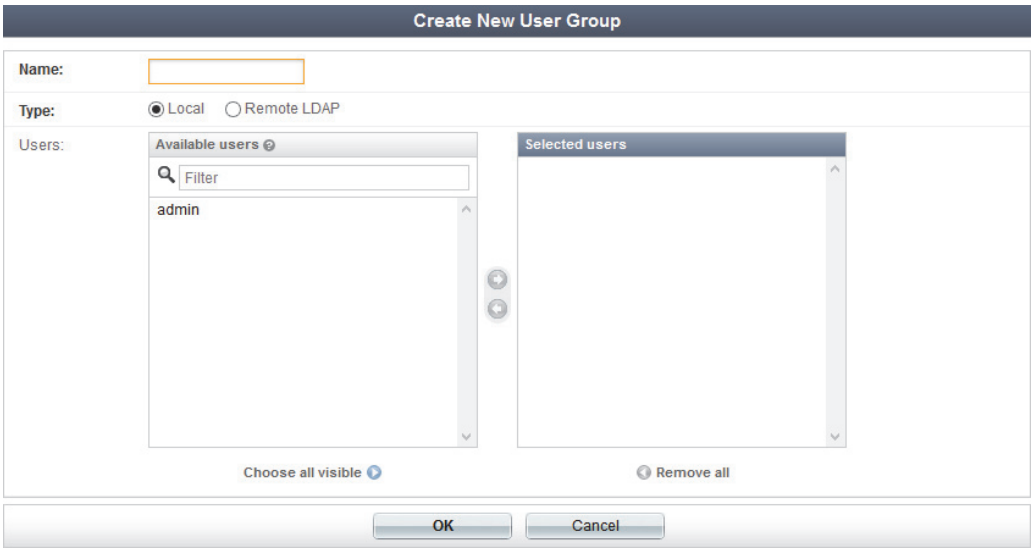
Users can be assigned to groups during user account configuration (see "Editing a user" on page 73), or by editing the groups to add users to it.

To view the user groups list, go to *Authentication* > *User Management* > *User Groups*.

To create a new user group:

1. Go to *Authentication* > *User Management* > *User Groups* and select *Create New*.
   The *Create New User Group* window opens.

Figure 60: Create a new user group



2. Enter the following information:

Name	Enter a name for the group.
Type	Select the type of group, either *Local* or *Remote LDAP*.
Users	Select users from the *Available users* box and move them to the *Selected users* box to add them to the group. This option is only available if *Type* is *Local*.
User retrieval	Determine group membership by selecting either *Specify an LDAP filter* or *Set a list of imported remote users*. This option is only available if *Type* is *Remote LDAP*.

Remote LDAP	Select a remote LDAP server from the drop-down list. At least one remote LDAP server must already be configured, see "Remote LDAP servers" on page 95. This option is only available if *Type* is *Remote LDAP*.
LDAP filter	Enter an *LDAP filter*. Optionally, select Test filter to ensure that the filter works as expected. This option is only available if *Type* is *Remote LDAP* and *User retrieval* is set to *Specify an LDAP filter*.
Remote users	Select remote users from the *Available remote users* box and move them to the *Selected remote users* box to add them to the remote group. This option is only available if *Type* is *Remote LDAP* and *User retrieval* is set to *Set a list of imported remote users*.

3. Select *OK* to create the new group.

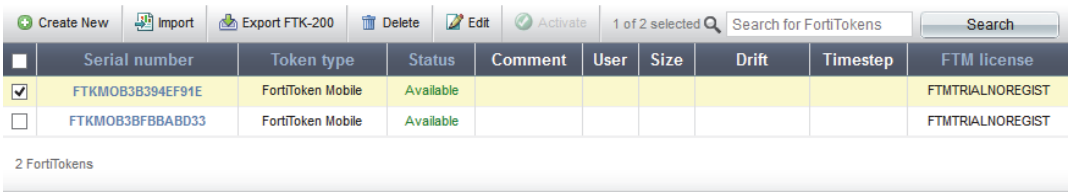
To edit a user group:

1. In the user group list, select the group that you need to edit.
2. Edit the settings as required. The settings are the same as when creating a new group.
3. Select *OK* to apply your changes.

FortiTokens

Go to *Authentication* > *User Management* > *FortiTokens* to view a list of configured FortiTokens. From here, FortiTokens can be added, imported, exported, edited, deleted, and activated. For more information, see "FortiToken devices and mobile apps" on page 86.

Figure 61: FortiTokens



The following information is shown:

Create New	Create a new FortiToken, see "To add FortiTokens manually:" on page 87.
Import	Import a list of FortiTokens, see "To import FortiTokens from a CSV file:" on page 87 and "To import FortiTokens from a FortiGate unit:" on page 88.
Export	Export the FortiToken list, see "To export FortiTokens:" on page 88.
Delete	Delete the selected FortiToken or FortiTokens.
Edit	Edit the selected FortiToken or FortiTokens.
Activate	Activate the selected FortiToken or FortiTokens.

Search	Enter a search term in the search field, then select *Search* to search the FortiToken list.
Serial number	The FortiToken's serial number.
Token type	The FortiToken type, either *FortiToken 200* or *FortiToken Mobile*.
Status	Whether or not the FortiToken is activated.
Comment	User comments.
User	The user to whom the FortiToken applies.
Size	The size of the token.
Drift	The time difference between the FortiAuthenticator and the FortiToken. For information on removing the drift, see "FortiToken drift adjustment" on page 89.
Timestep	The FortiToken timestep.
FTM License	The FTM license applied to the FortiToken.

MAC devices

Non-802.1X compliant devices can be identified and accepted onto the network using MAC address authentication. See "Non-compliant devices" on page 111 for more information.

RADIUS attributes

Some services can receive information about an authenticated user through RADIUS vendor-specific attributes. FortiAuthenticator user groups and user accounts can include RADIUS attributes for Fortinet and other vendors.

Attributes in user accounts can specify user-related information. For example, the *Default* attribute *Framed-IP-Address* specifies the VPN tunnel IP address to be sent to the user by the Fortinet SSL VPN.

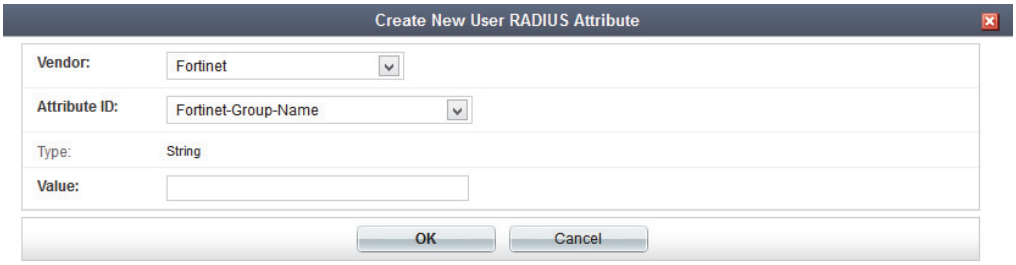
Attributes in user groups can specify more general information, applicable to the whole group. For example, specifying third-party vendor attributes to a switch could enable administrative level login to all members of the *Network_Admins* group, or authorize the user to the correct privilege level on the system.

To add RADIUS attributes to a user or group:

1. Go to *Authentication* > *User Management* > *Local Users* and select a user account to edit, or go to *Authentication* > *User Management* > *User Groups* and select a group to edit.
2. In the *RADIUS Attributes* section, select *Add Attribute*.

   The *Create New User Group RADIUS Attribute* or *Create New User RADIUS Attribute* window opens.

Figure 62: Create a new RADIUS attribute



3. Select the appropriate *Vendor* and *Attribute ID*, then enter the attribute's value in the *Value* field.
4. Select *OK* to add the new attribute to the user or group.
5. Repeat the above steps to add additional attributes as needed.

FortiToken devices and mobile apps

A FortiToken device is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit token passcode. FortiToken Mobile is an application for mobile devices that performs the same one-time password function as a FortiToken device.

Each FortiAuthenticator unit or virtual machine (VM) is supplied with two trial FortiToken Mobile tokens. To obtain the free FortiToken Mobile tokens (if they have not been created dynamically on install), select Get FortiToken Mobile trial tokens when adding a token (see "To add FortiTokens manually:" on page 87).

This may be required if, for example, you are upgrading an unlicensed FortiAuthenticator unit to a licensed one, as the old tokens associated with the unlicensed serial number will not be compatible with the new, licensed serial number. The tokens will still work, but they are not able to be reassigned to a new user. In this case, you must delete the old tokens, and then generate new ones.

If using a token passcode that is time-based, it is imperative that the FortiAuthenticator unit clock is accurate. If possible, configure the system time to be synchronized with an NTP server.

To perform token-based authentication, the user must enter the token passcode. If the user's username and password are also required, this is called two-factor authentication. The displayed code changes every 60 seconds.

The FortiToken device has a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. When not in use, the LCD screen is shut down to extend the battery life.

Do not put the FortiToken device on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and should be treated with similar care.

See "FortiTokens" on page 84 for more information.

FortiAuthenticator and FortiTokens

With FortiOS, FortiToken identifiers must be entered to the FortiGate unit, which then contacts FortiGuard servers to verify the information before activating them.

FortiAuthenticator acts as a repository for all FortiToken devices used on your network. It is a single point of registration and synchronization for easier installation and maintenance.

To register FortiTokens, you must have a valid FortiGuard connection. Otherwise, any FortiTokens you enter will remain in Inactive status. After the FortiTokens are registered, the connection to FortiGuard is no longer essential.

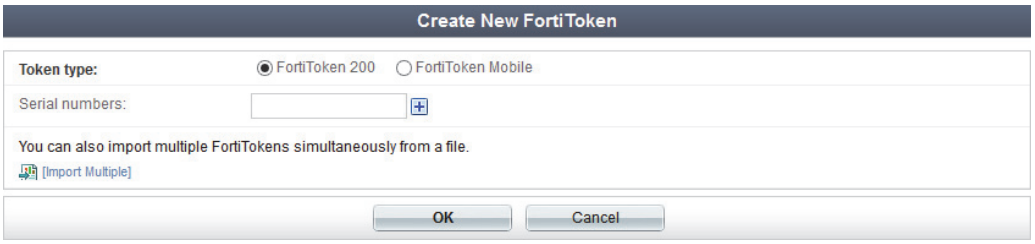
If a token authentication fails, check that the system time on the FortiAuthenticator unit is correct and then re-synchronize the FortiToken.

To add FortiTokens manually:

1. Go to *Authentication* > *User Management* > *FortiTokens* and select *Create New.*

   The *Create New FortiToken* window opens.

   Figure 63: New FortiToken



2. Select the *Token Type*, either *FortiToken 200* or *FortiToken Mobile*.
3. If *FortiToken 200* is selected as the *Token Type*, enter one or more token serial numbers in the *Serial numbers* field. You can also import multiple tokens by selecting *Import Multiple* (see "To import FortiTokens from a CSV file:" and "To import FortiTokens from a FortiGate unit:" on page 88).

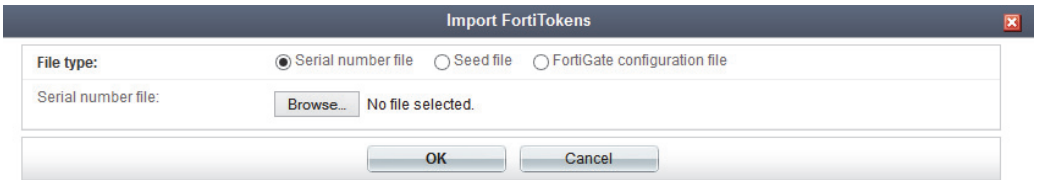
   If *FortiToken Mobile* is selected as the *Token Type*, enter the activation codes in the *Activation codes* field, or select *Get FortiToken Mobile free trial tokens* to use temporary tokens.
4. Select *OK* to add the FortiToken or FortiTokens.

To import FortiTokens from a CSV file:

1. From the FortiToken list, select *Import.*

   The *Import FortiTokens* window opens.

   Figure 64: Import FortiTokens



2. Do one of the following:
   - Select *Serial number file* to load a CSV file that contains token serial numbers for the tokens. (FortiToken devices have a barcode on them that can help you read serial numbers to create the import file.)
   - Select *Seed file* to load a CSV file that contains the token serial numbers, encrypted seeds, and IV values. (FortiToken devices have a barcode on them that can help you read serial numbers to create the import file.)
3. Select *Browse...*, find the configuration file, and select *Open*.
4. Select *OK* to import the FortiTokens.

To import FortiTokens from a FortiGate unit:

1. Export the FortiGate unit configuration to a file.
2. From the FortiToken list, select *Import*.
3. Select *FortiGate Configuration file*.

Figure 65: Import FortiTokens from a FortiGate

4. In the *Data to import* field, select *Import FortiToken 200 only*, *Import FortiToken 200 and only their associated users*, or Import all *FortiToken 200 and users*.
5. Select *Browse...*, find the configuration file, then select *Open*.
6. If the file is encrypted, enter the password in the *Password* field.
7. Select *OK* to import the FortiTokens.

To export FortiTokens:

1. From the FortiToken list, select *Export*.
2. Save the file to your computer.

Monitoring FortiTokens

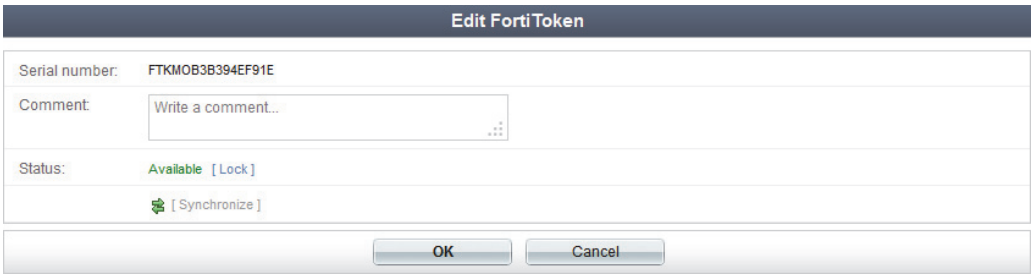
To monitor the total number of FortiToken devices registered on the FortiAuthenticator unit, as well as the number of disabled FortiTokens, go to *System* > *Dashboard* > *Status* and view the *User Inventory* widget (see “User Inventory widget” on page 40).

You can also view the list of FortiTokens, their status, if their clocks are drifting, and which user they are assigned to from the FortiToken list found at *Authentication* > *User Management* > *FortiTokens*, see “FortiTokens” on page 84.

FortiToken device maintenance

Go to *Authentication* > *User Management* > *FortiTokens*, then select the FortiToken on which you need to perform maintenance and select *Edit*.

Figure 66: Edit a FortiToken



The following actions can be performed:

- Comments can be added for FortiToken.
- The device can be locked if it has been reported lost or stolen:

  A reason for locking the device must be entered, and a temporary SMS token can be provided.
- The device can be unlocked if it is recovered.
- The device can be synchronized:

  Synchronize the FortiAuthenticator and the FortiToken device when the device clock has drifted. This ensures that the device provides the token code that the FortiAuthenticator unit expects, as the codes are time-based. Fortinet recommends synchronizing all new FortiTokens.
- The device history can be viewed, showing all commands applied to this FortiToken.

FortiToken drift adjustment

When the FortiAuthenticator unit and FortiTokens have been initialized prior to setting an NTP server, the time difference can be too large to correct with the synchronize function, forcing all tokens to resynchronize. To avoid this, selected tokens can be manually drift shifted.

The following procedure is intended to be used only in special cases where some FortiTokens are severely out-of-sync. Under normal circumstances, this is not required.

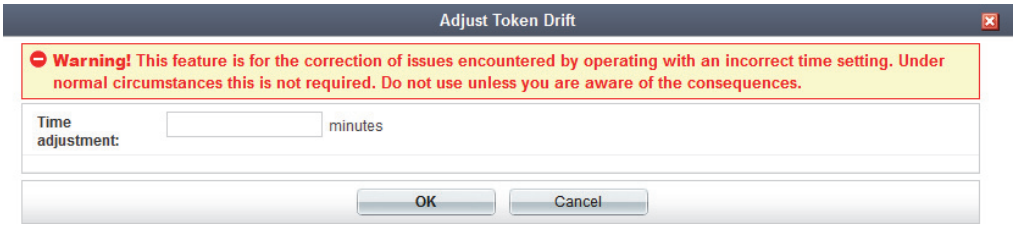
Only activated FortiTokens can be adjusted.

To perform time drift adjustment on a FortiToken:

1. In a browser, go to `https://<FortiAuthenticator_IP >/admin/fac_auth/fortitokendrift/`.
2. Select the FortiToken to adjust, then select *Adjust Drift*.

   The *Adjust Token Drift* window opens.

Figure 67: Adjust token drift



3. Enter the required *Time adjustment* in minutes.

   Include a minus sign for a negative value, but don't use a plus sign for a positive value.
4. Select *OK* to adjust the token drift.

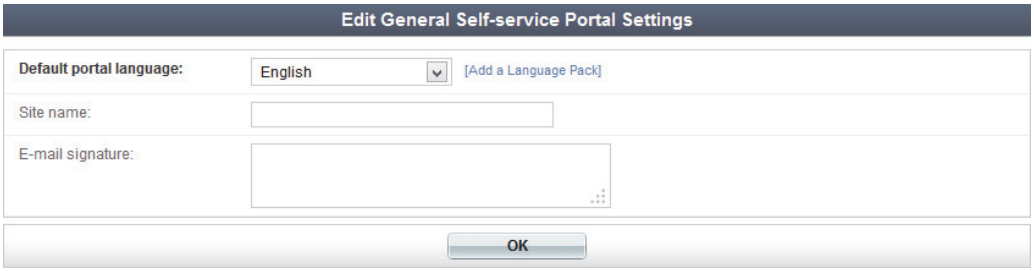
Self-service portal

The self-service portal provides options for configuring general self-service portal options, self-registration options, replacement messages, and device self-enrollment settings.

General

To configure general self-service portal settings, go to *Authentication* > *Self-service Portal* > *General*.

Figure 68: General self-service portal settings



The following settings can be adjusted:

Default portal language	Select a default portal language from the drop-down list.
Add a Language Pack	Select to add a language pack. Several languages are included by default. A translation pack can be obtained from Fortinet support if you need to translate to your local language.
Site name	Enter a name that is used when referring to this site. If left blank, the default name will be the site DNS domain name or IP address.
E-mail Signature	Add a signature to be appended to the end of outgoing email messages.

Self-registration

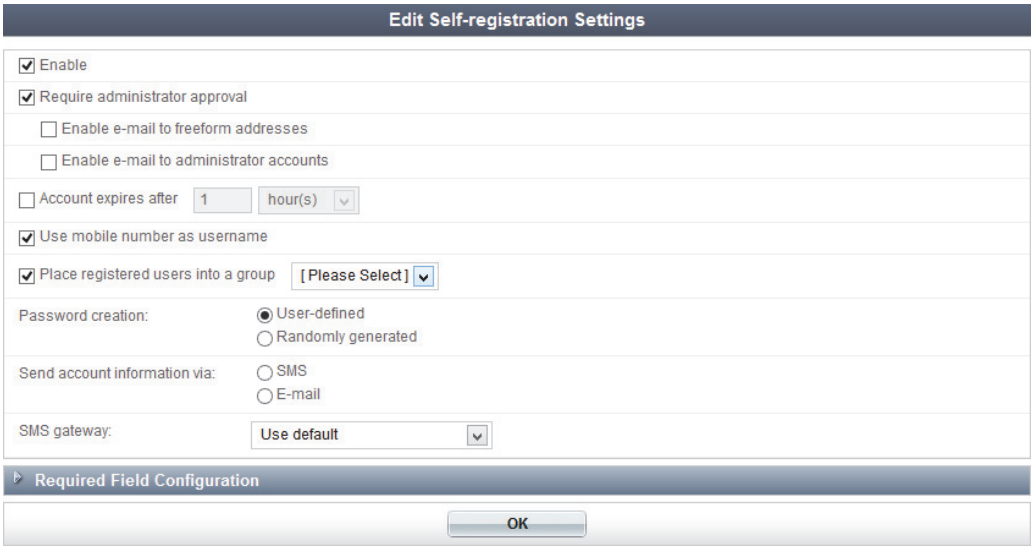
When self-registration is enabled, users can request registration through the FortiAuthenticator login page. Self-registration can be configured so that a user request is emails to the device administrator for approval.

When the account is ready for use, the user receives an email or SMS message with their account information.

To enable self-registration:

1. Go to *Authentication* > *Self-service Portal* > *Self Registration*.

Figure 69: User self-registration



2. Select *Enable* to enable self-registration.
3. Optionally, configure the following settings:

Require administrator approval	Select to require that an administrator approves the user.
Enable e-mail to freeform addresses	Select to send self-registration requests to the email addresses entered in the *Administrator e-mail addresses* field.
Enable e-mail to administrator accounts	Select to send self-registration requests to specific administrators. Select the required administrators from the *Available administrators* box and move them to the *Chosen administrators* box.
Account expires after	Select to specify how long until self-generated accounts will be deleted after they are generated.
Use mobile number as username	If enabled, after a successful registration, the user's password will be sent to them via SMS to confirm their identity.
Place registered users into a group	Select a group into which self-registered users will be placed from the drop-down list.
Password creation	Select how a password is created, either *User-defined* or *Randomly generated*.

Send account information via	Choose how to send account information to the user, either *SMS*, *E-mail*, or *Display on browser page*. The *Display on browser page* option is only available if administrator approval is not required.
SMS gateway	Select an SMS gateway from the drop-down list. See "SMS Gateways" on page 61 for more information.
Required Field Configuration	Select the fields that the user is required to populate when self-registering. Options include: *First name*, *Last name*, *E-mail, address*, *Address*, *City*, *State/Province*, *Country*, *Phone number*, *Mobile number*, *Custom field 1*, *Custom field 2*, and *Custom field 3*. For information about custom fields, see "Custom user fields" on page 69.

4. Select *OK* to apply your changes.

To approve a self-registration request:

1. Select the link in the *Approval Required for...* email message to open the *New User Approval* page in your web browser.
2. Review the information and select either *Approve* or *Deny*, as appropriate.

   Approval is required only if *Require administrator approval* is enabled in the self-registration settings.

   If the request is approved, the FortiAuthenticator unit sends the user an email or SMS message stating that the account has been activated.

How a user requests registration

A user can request registration, or self-register, from the FortiAuthenticator login screen.

To request registration:

1. Browse to the IP address of the FortiAuthenticator unit.

   Security policies must be in place on the FortiGate unit to allow these sessions to be established.
2. Select *Register* to open the user registration page.
3. Fill in all the required fields and, optionally, fill in the *Additional Information* fields
4. Select *OK*. to request registration.

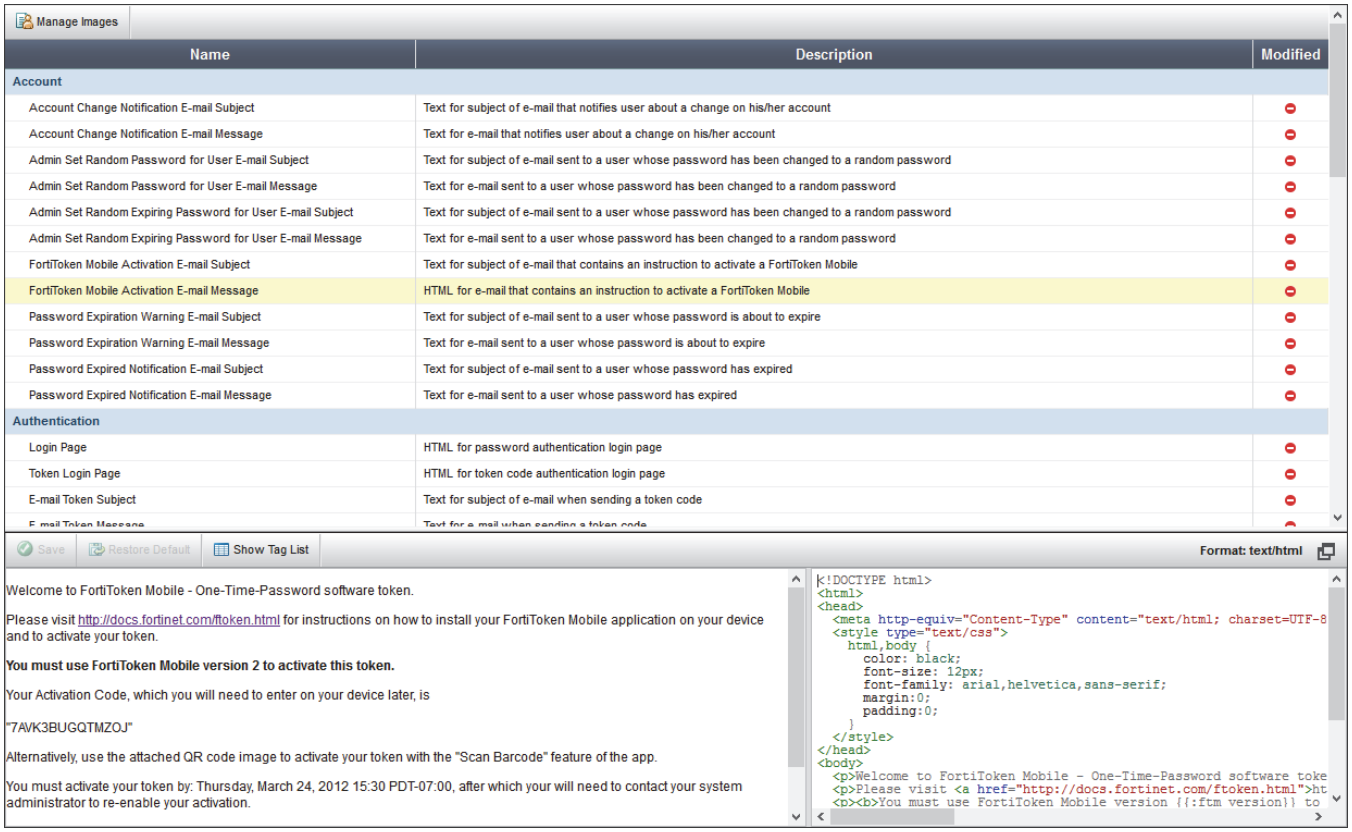
   If administrator approval is not required and *Display on browser page* is enabled, the account details are immediately displayed to the user.

Replacement message

The replacement messages list enables you to view and customize replacement messages, and manage images.

Go to *Authentication* > *Self-service Portal* > *Replacement Message* to view the replacement message list.

Figure 70: Replacement message list



The replacement messages are split into five categories: *Account*, *Authentication*, *Device Certificate Enrollment*, *Password Reset*, and *User Registration*.

Selecting a specific message will display the text and HTML or plain text of the message in the lower half of the content pane.

Selecting *Show Tag List* will display a table of the tags used for that message atop the message's HTML or plain text box.

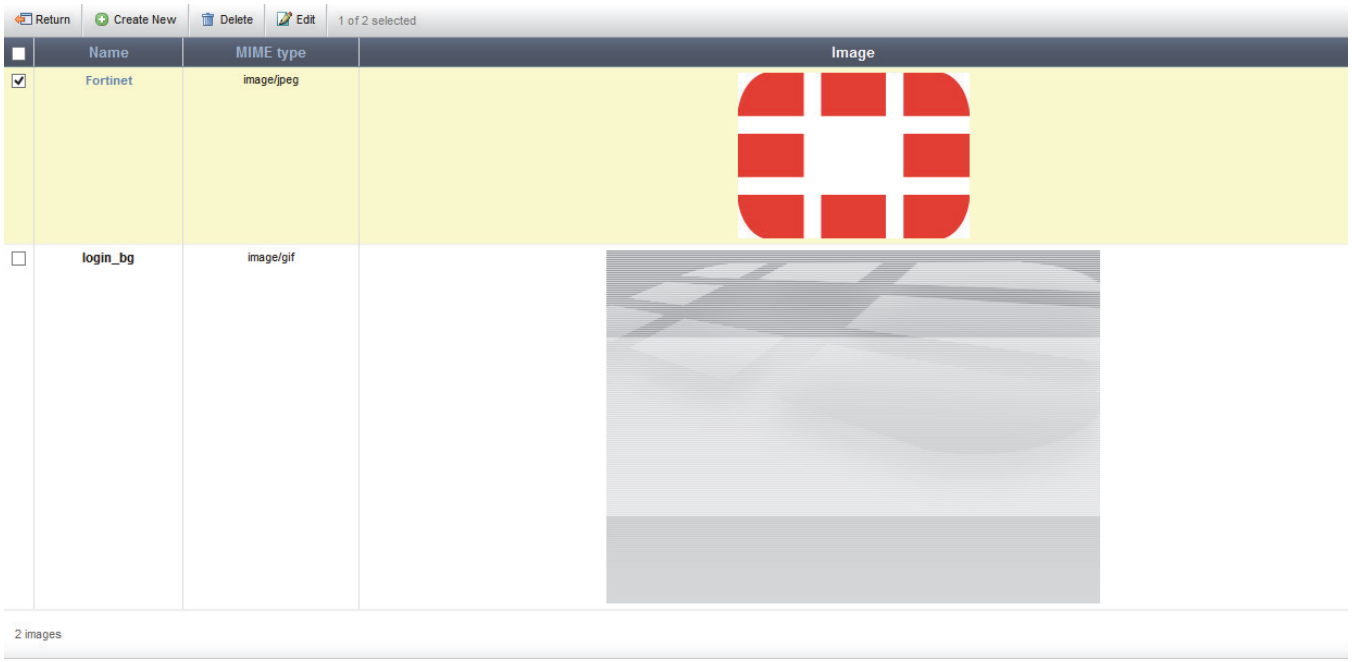
To edit a replacement message:

1. Select a message in the replacement message list.
2. Edit the plain text or HTML code in the lower right pane, or select the open in new window icon, , to edit the message in a new browser window.
3. When you are finished editing the message, select *Save* to save your changes.
4. If you have made an error when editing the message, select *Restore Default* to restore the message to its default value.

Manage Images

Images can be managed by selecting *Manage Images* in the *Replacement Message* window.

Figure 71: Manage images



Select *Return* to return to the replacement messages screen. Images can also be added, deleted, and edited.

To add an image:

1. In the manage images screen, select *Create New* to open the *Create New Image* window.
2. Enter a name for the image in the *Name* field.
3. Select *Browse...*, find the GIF, JPEG, or PNG image file that you are adding, and then select *Open*.

   The maximum image size is 65kB.
4. Select OK to add the image.

To delete an image:

1. In the manage images screen, select an image, then select *Delete*.
2. Select *Yes, I'm sure* in the confirmation window to delete the image.

To edit an image:

1. In the manage images screen, select an image, then select *Edit*.
2. In the *Edit Image* window, edit the image name and file as required.
3. Select *OK* to apply your changes.

Device self-enrollment

Device certificate self-enrollment is a method for users to obtain certificates for their devices. It is primarily used in enabling EAP-TLS for Bring your own device (BYOD). For more information, see "Device self-enrollment" on page 110.

Remote LDAP servers

If you already have an LDAP server or servers configured on your network, FortiAuthenticator can connect to them for remote authentication, much like FortiOS remote authentication.

Adding a remote LDAP server

If you have existing LDAP servers, you may choose to continue using them with FortiAuthenticator by configuring them as remote LDAP servers.

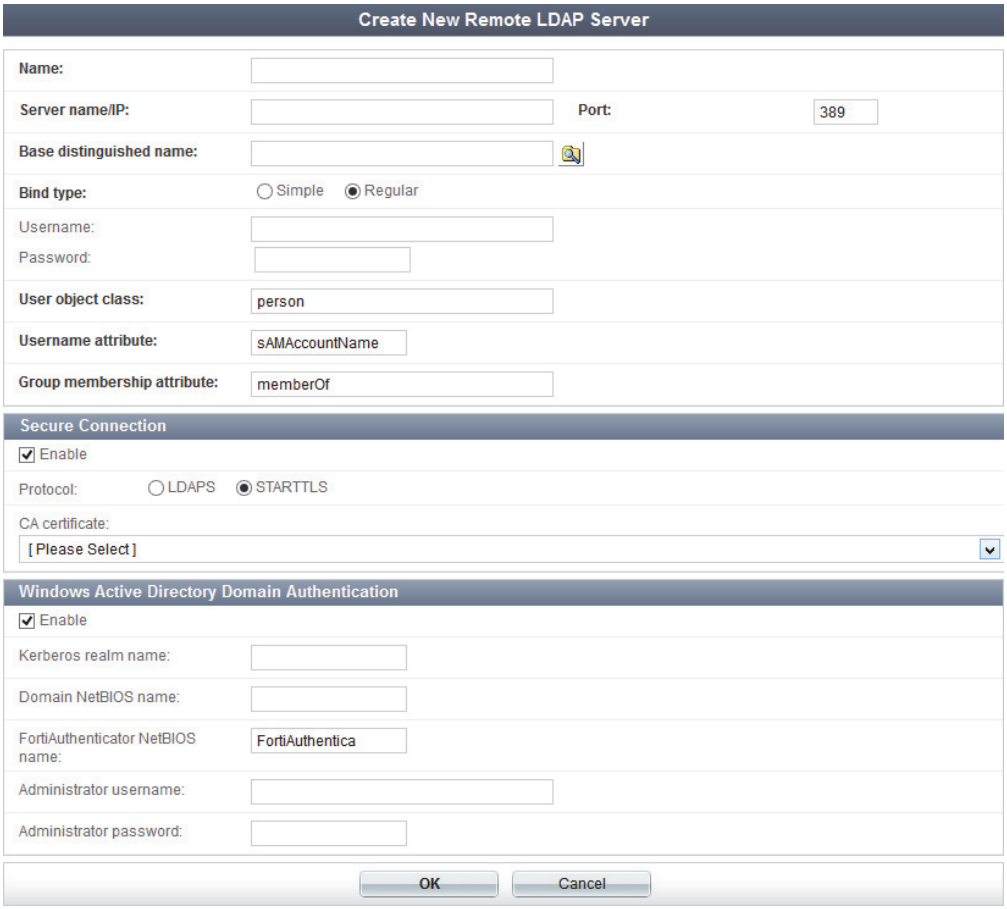
When entering the remote LDAP server information, if any information is missing or in the wrong format, error messages will highlight the problem for you.

To add a remote LDAP server entry:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and select *Create New*.

   The *Create New Remote LDAP Server* window opens.

Figure 72: Add an LDAP server



2. Enter the following information.

Name	Enter the name for the remote LDAP server on FortiAuthenticator.
Server name/IP	Enter the IP address or FQDN for this remote server.
Port	Enter the port number.
Base distinguished name	Enter the base distinguished name for the server using the correct X.500 or LDAP format. The maximum length of the DN is 512 characters. You can also select the browse button to view and select the DN on the LDAP server.
Bind Type	The Bind Type determines how the authentication information is sent to the server. Select the bind type required by the remote LDAP server. • *Simple*: bind using the user's password which is sent to the server in plaintext without a search. • *Regular*: bind using the user's DN and password and then search. If the user records fall under one directory, you can use *Simple* bind type. But *Regular* is required to allow a search for a user across multiple domains.
User object class	The type of object class to search for a user name search. The default is *person*.
Username attribute	The LDAP attribute that contains the user name. The default is *sAMAccountName*.
Group membership attribute	Used as the attribute to search for membership of users or groups in other groups.

3. If you want to have a secure connection between the FortiAuthenticator unit and the remote LDAP server, under *Secure Connection*, select *Enable*, then enter the following:

Protocol	Select *LDAPS* or *STARTLS* as the LDAP server requires.
CA Certificate	Select the CA certificate that verifies the server certificate from the drop-down list.

4. If you want to authenticate users using MSCHAP2 PEAP in an Active Directory environment, enable *Windows Active Directory Domain Authentication*, then enter the required Windows AD Domain Controller information.

   When you are finished here, go to *Authentication* > *RADIUS Service* > *Clients* to choose whether authentication is available for all Windows AD users or only for Windows AD users who belong to particular user groups that you select. See "Adding a RADIUS authentication client" on page 97 for more information.

5. Select *OK* to apply your changes.

   You can now add remote LDAP users, as described in "Remote users" on page 79.

Adding a RADIUS authentication client

Before the FortiAuthenticator unit can accept RADIUS authentication requests from a FortiGate unit, the FortiGate unit must be registered as a authentication client on the FortiAuthenticator unit.

The FortiAuthenticator RADIUS server is already configured and running with default values. Each user account on the FortiAuthenticator unit has an option to authenticate the user using the RADIUS database.

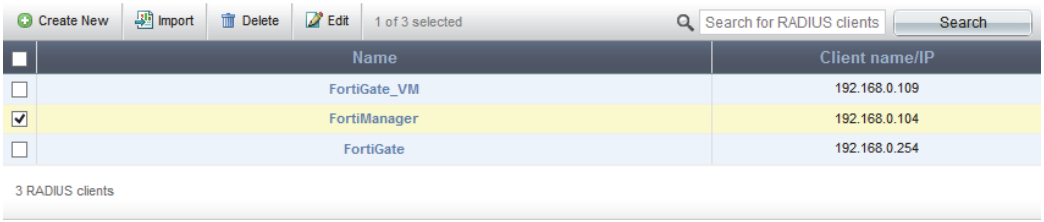
Every time there is a change to the list of RADIUS authentication clients, two log messages are generated: one for the client change, and one to state that the RADIUS server was restarted to apply the change.

FortiAuthenticator unit allows both RADIUS and remote LDAP authentication for RADIUS authentication client entries. If you want to use a remote LDAP server, you must configure it first so that you can be select it in the RADIUS authentication client configuration, see "Remote LDAP servers" on page 95. You can configure the built-in LDAP server before or after creating client entries, see "LDAP service" on page 100.

To configure a RADIUS accounting client:

1. Go to *Authentication* > *RADIUS Service* > *Clients* to view the RADIUS client list.

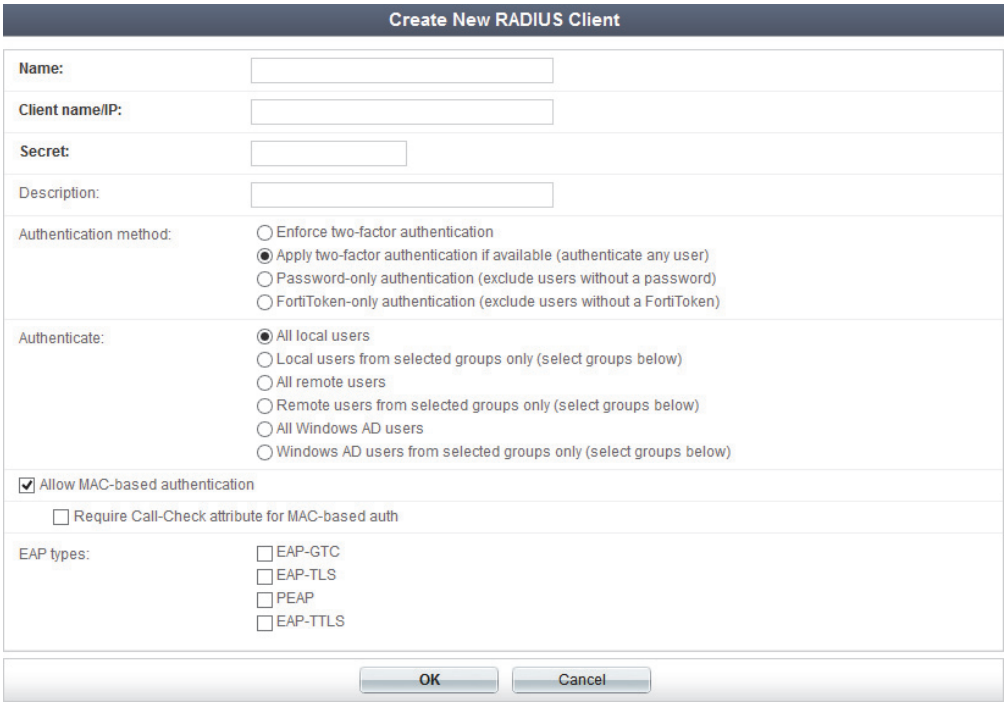
Figure 73:RADIUS client list



2. Select *Create New* to add a new RADIUS client.

   The *Create New RADIUS Client* window opens.

Figure 74: New RADIUS client



3. Enter the following information:

Name	A name to identify the FortiGate unit.
Client name/IP	The FQDN or IP address of the unit.
Secret	The RADIUS passphrase that the FortiGate unit will use.
Description	Optionally, enter information about the FortiGate unit.
Authentication method	Select one of the following: • Enforce two-factor authentication • Apply two-factor authentication if available (authenticate any user) • Password-only authentication (exclude users without a password) • FortiToken-only authentication (exclude users without a FortiToken)
Authenticate	Limit who can authenticate.
All local users	Authenticate any of the configured local users.
Local users from selected groups only	Authenticate only members of specific FortiAuthenticator user groups. Add the required user groups to the *Selected local user groups* list.
All remote users	Authenticate only users of the remote LDAP server selected from the *Remote LDAP server* drop-down list.

Remote users from selected groups only	Authenticate only users of specific groups on the selected *Remote LDAP server*. If the server is not listed, create it. See "Remote LDAP servers" on page 95. Add the required user groups to the *Selected remote user groups* list.
All Windows AD users	This is available if Windows Active Directory Domain Authentication is enabled for the domain controller in *Authentication* > *Remote Auth. Servers* > *LDAP*, see "Remote LDAP servers" on page 95.
Windows AD users from selected groups only	This is available if Windows Active Directory Domain Authentication is enabled for the domain controller in *Authentication* > *Remote Auth. Servers* > *LDAP*. In *Remote LDAP server*, select the desired remote user groups.
Allow MAC-based authentication	To allow 802.1X authentication for non-interactive devices, FortiAuthenticator can identify and bypass authentication for a device based on its MAC address. This is used for devices that do not allow the usual username or password input to perform 802.1X authentication, such as network printers. Enter these units in *Authentication* > *User Management* > *MAC Devices*. For more information, see "MAC devices" on page 85.
Require Call-Check attribute for MAC-based auth	The FortiAuthenticator unit expects the username and password attributes to be set to the source MAC address. This option also requires a Service-Type attribute set to *Call Check* and a Calling-Station-Id attribute set to the source MAC address.
EAP types	Select the 802.1X EAP authentication types to accept. If you require mutual authentication, select EAP-TLS. For more information, see "EAP" on page 107.

4. Select *OK* to add the new RADIUS client.

If authentication is failing, check that the authentication client is configured and that its IP address is correctly specified. Common causes of problems are:

- RADIUS packets being sent from an unexpected interface
- NAT being performed between the authentication client and the FortiAuthenticator unit.

Importing authentication clients

Authentication client information can be imported as a CSV file by selecting *Import* in the from the RADIUS client list.

The CSV file has one record per line, with the record format: client name (32 characters max), FQDN or IP address (128 characters max), secret (optional, 63 characters max).

Extensible authentication protocol

The FortiAuthenticator unit supports several IEEE 802.1X EAP methods. EAP settings can be configured from *Authentication* > *RADIUS Service* > *EAP*. See "EAP" on page 107 for more information.

LDAP service

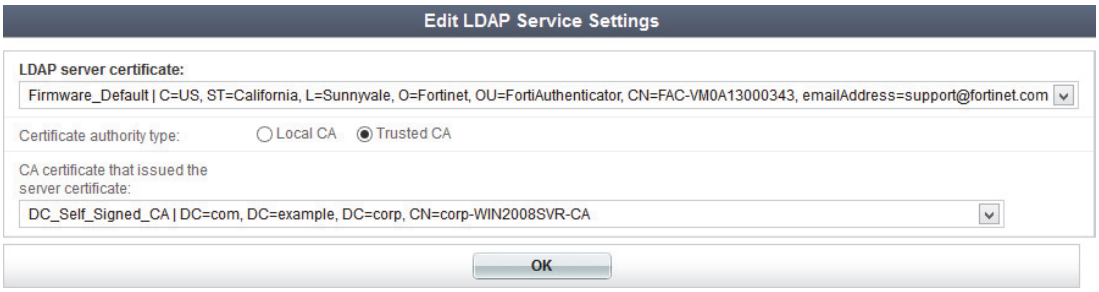
LDAP is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

In the LDAP protocol there are a number of operations a client can request such as search, compare, and add or delete an entry. Binding is the operation where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on that user's permissions.

General

To configure general LDAP service settings, go to *Authentication* > *LDAP Service* > *General*.

Figure 75: General LDAP service settings



LDAP server certificate	Select the certificate that the LDAP server will present from the drop-down list.
Certificate authority type	Select either *Local CA* or *Trusted CA*.
CA certificate that issued the server certificate	Select the CA certificate that issued the server certificate from the drop-down list.

Select *OK* to apply any changes that you have made.

Directory tree overview

The LDAP tree defines the hierarchical organization of user account entries in the LDAP database. The FortiGate unit requesting authentication must be configured to address its request to the right part of the hierarchy.

An LDAP server's hierarchy often reflects the hierarchy of the organization it serves. The root represents the organization itself, usually defined as Domain Component (DC), a DNS domain, such as `example.com` (as the name contains a dot, it is written as two parts separated by a comma: `dc=example,dc=com`). Additional levels of hierarchy can be added as needed. These include:

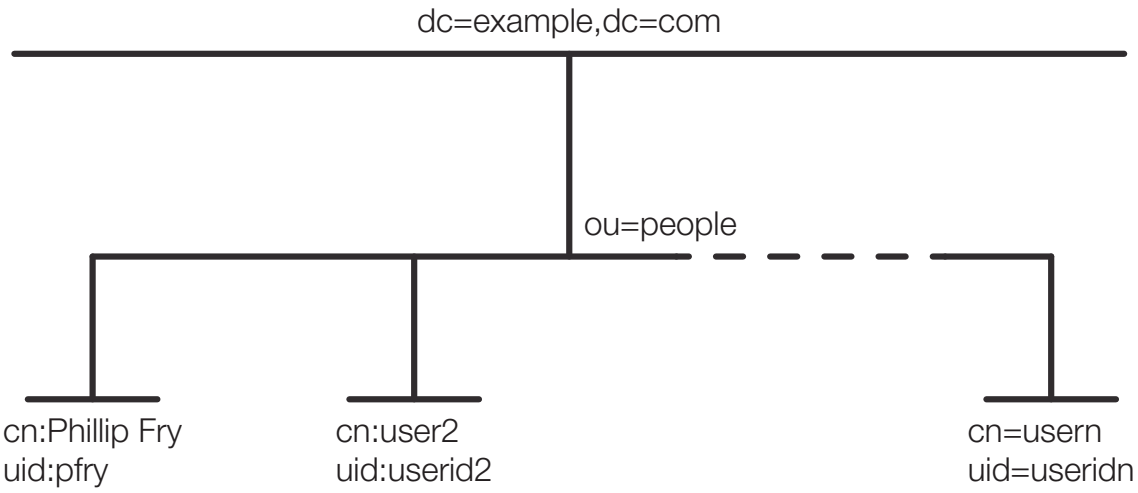
- Country (c)
- User Group (cn)
- User (uid)
- Organization (o)
- Organizational Unit (ou)

The user account entries relevant to user authentication will have element names such as UID (user ID) or CN (common name, the user's name). They can each be placed at their appropriate place in the hierarchy.

Complex LDAP hierarchies are more common in large organizations where users in different locations and departments have different access rights. For basic authenticated access to your office network or the Internet, a much simpler LDAP hierarchy is adequate.

The following is a simple example of an LDAP hierarchy in which the all user account entries reside at the Organization Unit (OU) level, just below DC.

Figure 76:LDAP object directory



When requesting authentication, an LDAP client, such as a FortiGate unit, must specify the part of the hierarchy where the user account record can be found. This is called the Distinguished Name (DN). In the above example, DN is `ou=People,dc=example,dc=com`.

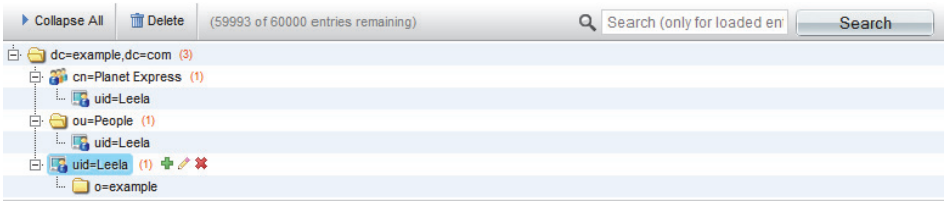
The authentication request must also specify the particular user account entry. Although this is often called the Common Name (CN), the identifier you use is not necessarily CN. On a computer network, it is appropriate to use UID, the person's user ID, as that is the information that they will provide at logon.

Creating the directory tree

The following sections provide a brief explanation of each part of the LDAP attribute directory, what is commonly used for representation, and how to configure it on FortiAuthenticator.

When an object name includes a space, as in *Test Users*, you have to enclose the text with double-quotes. For example: *cn="Test Users",cn=Builtin,dc=get,dc=local*.

Figure 77:LDAP directory tree example



Editing the root node

The root node is the top level of the LDAP directory. There can be only one. All groups, OUs, and users branch off from the root node. Choose a DN that makes sense for your organization's root node.

There are three common forms of DN entries:

The most common consists of one or more DC elements making up the DN. Each part of the domain has its own DC entry. This comes directly from the DNS entry for the organization. For example, for example.com, the DN entry is `"dc=example,dc=com"`.

Another popular method is to use the company's Internet presence as the DN. This method uses the domain name as the DN. For example, for example.com, the DN entry would be `"o=example.com"`.

An older method is to use the company name with a country entry. For example, for Example Inc. operating in the United States, the DN would be `o="Example, Inc.",c=US`. This makes less sense for international companies.

When you configure FortiGate units to use the FortiAuthenticator unit as an LDAP server, you will specify the distinguished name that you created here. This identifies the correct LDAP structure to reference.

To rename the root node:

1. Go to *Authentication* > *LDAP Service* > *Directory Tree*.
2. Select `dc=example,dc=com` to edit the entry.
3. In the *Distinguished Name (DN)* field, enter a new name.

   Example: `"dc=fortinet,dc=com"`.
4. Select *OK* to apply your changes.

If your domain name has multiple parts to it, such as shiny.widgets.example.com, each part of the domain should be entered as part of the DN: `dc=shiny,dc=widgets,dc=example,dc=com`, for example.

Adding nodes to the LDAP directory tree

You can add a subordinate node at any level in the hierarchy as required.

To add a node to the tree:

1. From the LDAP directory tree, select the green plus symbol next to the DN entry where the node will be added.

   The *Create New LDAP Entry* window opens.

   Figure 78: New LDAP directory tree entry

2. In the *Class* field, select the identifier to use.

   For example, to add the `ou=People` node from the earlier example, select *Organizational Unit (ou)*.
3. Select the required value from the drop-down list, or select *Create New* to create a new entry of the selected class.
4. Select *OK* to add the node.

Nodes can be edited after creation by selecting the edit, or pencil, icon next to the node name.

Adding user accounts to the LDAP tree

You must add user account entries at the appropriate place in the LDAP tree. These users must already be defined in the FortiAuthenticator user database. See “Adding a user” on page 72.

To add a user account to the tree:

1. From the LDAP directory tree, expand nodes as needed to find the required node, then select the node’s green plus symbol.

   In the earlier example, you would do this on the `ou=People` node.
2. In the *Class* field, select *User (uid)*.

   The list of available users is displayed. You can choose to display them alphabetically by either user group or user.
3. Select the required users in the *Available Users* box and move them to the *Chosen Users* box.
4. Select *OK* to add the user account to the tree.

You can verify your users were added by expanding the node to see their UIDs listed below it.

Moving LDAP branches in the directory tree

At times you may want to rearrange the hierarchy of the LDAP structure. For example a department may be moved from one country to another.

While it is easy to move a branch in the LDAP tree, all systems that use this information will need to be updated to the new structure or they will not be able to authenticate users.

To move an LDAP branch:

1. From the LDAP directory tree, select *Expand All* and find the branch that is to be moved.
2. Click and drag the branch from its current location to its new location

   When the branch is hovered above a valid location, an arrow will appear to the left of the current branch to indicate where the new branch will be inserted. It will be inserted below the entry with the arrow.

Removing entries from the directory tree

Adding entries to the directory tree involves placing the attribute at the proper place. However, when removing entries it is possible to remove multiple branches at one time.

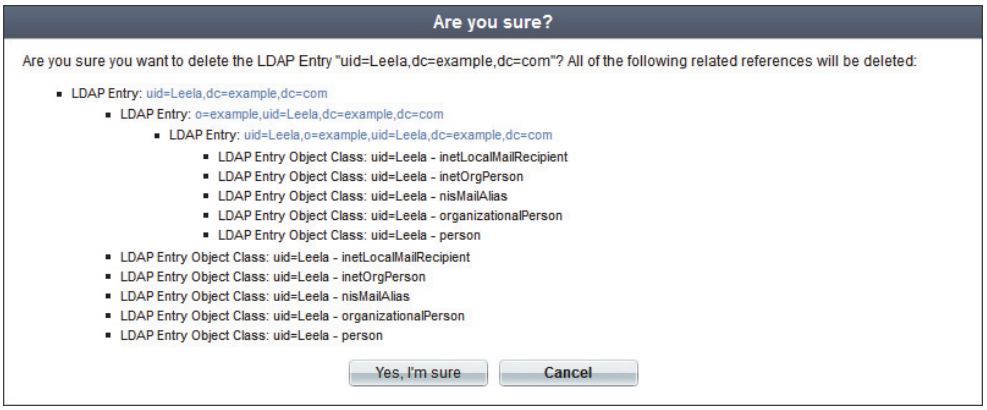
Take care not to remove more branches than you intend. Remember that all systems using this information will need to be updated to the new structure or they will not be able to authenticate users.

To remove an entry from the LDAP directory tree:

1. From the LDAP directory tree, select *Expand All* and find the branch that is to be removed.
2. Select the red X to the right of the entry name.

   You will be prompted to confirm your deletion. Part of the prompt displays the message of all the entries that will be removed with this deletion. Ensure this is the level that you intend to delete.

Figure 79: Are you sure?



3. Select *Yes, I'm sure* to delete the entry.

If the deletion was successful there will be a green check next to the successful message above the LDAP directory and the entry will be removed from the tree.

Configuring a FortiGate unit for FortiAuthenticator LDAP

When you have defined the FortiAuthenticator LDAP tree, you can configure FortiGate units to access the FortiAuthenticator as an LDAP server and authenticate users.

To configure the FortiGate unit for LDAP authentication:

1. On the FortiGate unit, go to *User & Device* > *Authentication* > *LDAP Server* and select *Create New*.
2. Enter the following information:

Name	Enter a name to identify the FortiAuthenticator LDAP server on the FortiGate unit.
Server Name / IP	Enter the FQDN or IP address of the FortiAuthenticator unit.
Server Port	Leave at default (389).
Common Name Identifier	Enter `uid`, the user ID.
Distinguished Name	Enter the LDAP node where the user account entries can be found. For example, `ou=People,dc=example,dc=com`
Bind Type	The FortiGate unit can be configured to use one of three types of binding: • anonymous - bind using anonymous user search • regular - bind using username/password and then search • simple - bind using a simple password authentication without a search You can use simple authentication if the user records all fall under one distinguished name (DN). If the users are under more than one DN, use the anonymous or regular type, which can search the entire LDAP database for the required username. If your LDAP server requires authentication to perform searches, use the regular type and provide values for *User DN* and *Password*.
Secure Connection	If you select *Secure Connection*, you must select LDAPS or STARTTLS protocol and the CA security certificate that verifies the FortiAuthenticator unit's identity. If you select LDAPS protocol, the Server Port will change to 636.

3. Select *OK* to apply your settings.
4. Add the LDAP server to a user group. Specify that user group in identity-based security policies where you require authentication.

FortiAuthenticator agent

FortiAuthenticator Agent for Microsoft Windows is a credential provider plugin that allows a FortiToken OTP, validated by FortiAuthenticator, to be inserted into the Windows authentication process.

To download the FortiAuthenticator Agent, go to *Authentication* > *FortiAuthenticator Agent* > *Download*, and download the FortiAuthenticator Agent installer.

For more information about the FortiAuthenticator Agent, see the *FortiAuthenticator Agent for Microsoft Windows Administration Guide*, available from http://docs.fortinet.com/fauth.html.

Port-based Network Access Control

Port-based Network Access Control (PNAC), or 802.1X, authentication requires a client, an authenticator, and an authentication server (such as a FortiAuthenticator device).

The client is a device that wants to connect to the network. The authenticator is simply a network device, such as a wireless access point or switch. The authentication server is usually a host that supports the RADIUS and EAP protocols.

The client is not allowed access to the network until the client's identity has been validated and authorized. Using 802.1X authentication, the client provides credentials to the authenticator, which the authenticator forwards to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is allowed access to the network.

FortiAuthenticator supports several IEEE 802.1X EAP methods.

EAP

The FortiAuthenticator unit supports several IEEE 802.1X EAP methods. These include authentication methods most commonly used in WiFi networks.

EAP is defined in RFC 3748 and updated in RFC 5247. EAP does not include security for the conversation between the client and the authentication server, so it is usually used within a secure tunnel technology such as TLS, TTLS, or MS-CHAP.

The FortiAuthenticator unit supports several EAP methods:

Table 7: FortiAuthenticator-supported EAP methods

Method	Server Auth	Client Auth	Encryption	Native OS
PEAP (MSCHAPv2)	Yes	Yes	Yes	Windows XP, Vista, 7
EAP-TTLS	Yes	No	Yes	Windows Vista, 7
EAP-TLS	Yes	Yes	Yes	Windows (XP, 7), Mac OS X, iOS, Linux, Android

In addition to providing a channel for user authentication, EAP methods, except EAP-MD5, also provide certificate-based authentication of the server computer. EAP-TLS provides mutual authentication: the client and server authenticate each other using certificates. This is essential for authentication onto an enterprise network in a Bring Your Own Device (BYOD) environment.

For successful EAP-TLS authentication, the user's certificate must be bound to their account in *Authentication* > *User Management* > *Local Users* (see "Local users" on page 71) and the relevant RADIUS client in *Authentication* > *RADIUS Service* > *Clients* (see "Adding a RADIUS authentication client" on page 97) must permit that user to authenticate. By default, all local users can authenticate, but it is possible to limit authentication to specified user groups.

The FortiAuthenticator unit and EAP

A FortiAuthenticator unit delivers all of the authentication features required for a successful EAP-TLS deployment, including:

- Certificate Management: create and revoke certificates as a CA. See "Certificate Management" on page 135.
- SCEP Server: exchange a CSR and the resulting signed certificate, simplifying the process of obtaining a device certificate.
- RADIUS AAA server: act as an authentication, authorization, and accounting (AAA) server.

FortiAuthenticator unit configuration

To configure the FortiAuthenticator unit, you need to:

1. Create a CA certificate for the FortiAuthenticator unit. See "Certificate authorities" on page 143.

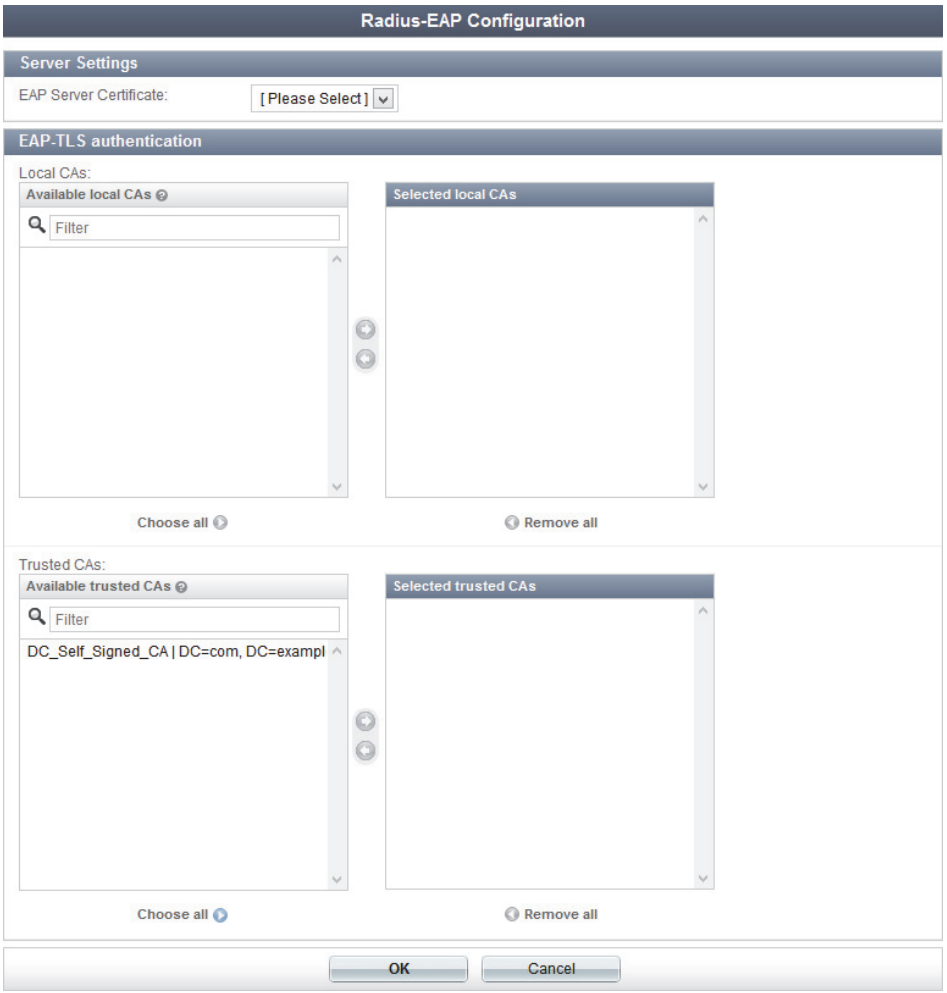
   Optionally, you can skip this step and use an external CA certificate instead. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* to import CA certificates. See "Trusted CAs" on page 151.
2. Create a server certificate for the FortiAuthenticator unit, using the CA certificate you created or imported in the preceding step. See "End entities" on page 136.
3. If you configure EAP-TTLS authentication, go to *Authentication* > *RADIUS Service* > *EAP* and configure the certificates for EAP. See "Configuring certificates for EAP" on page 109.
4. If SCEP will be used:
   a. Configure an SMTP server to be used for sending SCEP notifications. Then configure the email service for the administrator to use the SMTP server that you created. See "E-mail Services" on page 59.
   b. Go to *Certificate Management* > *SCEP* > *General* and select *Enable SCEP*. Then select the CA certificate that you created or imported in Step 1 in the *Default CA* field and select *OK*. See "SCEP" on page 152.
5. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and add the remote LDAP server that contains your user database. See "Adding a remote LDAP server" on page 95.
6. Import users from the remote LDAP server. You can choose which specific users will be permitted to authenticate. See "Remote users" on page 79.
7. Go to *Authentication* > *RADIUS Service* > *Clients* to add the FortiGate wireless controller as an authentication client. Be sure to select the type of EAP authentication you intend to use. See "Adding a RADIUS authentication client" on page 97.

Configuring certificates for EAP

The FortiAuthenticator unit can authenticate itself to clients with a CA certificate.

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* to import the certificate you will use.
2. Go to *Authentication* > *RADIUS Service* > *EAP*.

Figure 80:RADIUS EAP configuration



3. Select the EAP server certificate from the *EAP Server Certificate* drop-down list.
4. Select the trusted CAs and local CAs to use for EAP authentication from their requisite lists.
5. Select *OK* to apply the settings.

Configuring switches to use 802.1X authentication

The 802.1X configuration will be largely vendor dependent. The key requirements are:

- *RADIUS Server IP*: This is the IP address of the FortiAuthenticator
- *Key*: The preshared secret configured in the FortiAuthenticator authentication client settings
- *Authentication Port*: By default, FortiAuthenticator listens for authentication requests on port 1812.

Device self-enrollment

Device certificate self-enrollment is a method for local and remote users to obtain certificates for their devices. It is primarily used in enabling EAP-TLS for Bring your own device (BYOD). For example:

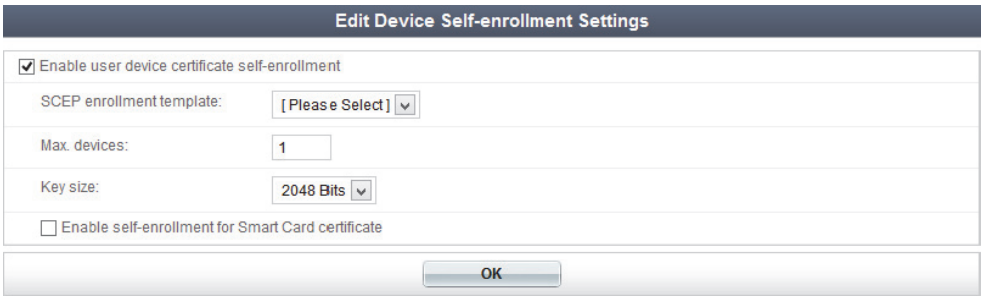
- A user brings their tablet to a BYOD organization.
- They log in to the FortiAuthenticator unit and create a certificate for the device.
- With their certificate, username, and password they authenticate to the wireless network.
- Without the certificate, they are unable to access the network.

EAP-TLS is a bidirectional certificate authentication method: the client and the FortiAuthenticator EAP need to have matching certificates from the same CA.

To enable device self-enrollment and adjust self-enrollment settings, go to *Authentication* > *Self-service Portal* > *Device Self-enrollment* and select *Enable user device certificate self-enrollment*.

SCEP must be enabled to activate this feature, see “SCEP” on page 152.

Figure 81: Edit device self-enrollment settings.



The following settings can be configured:

SCEP enrollment template	Select a SCEP enrollment template from the drop-down list. SCEP can be configured in *Certificate Management* > *SCEP*. See “SCEP” on page 152 for more information.
Max. devices	Set the maximum number of devices that a user can self-enroll.
Key size	Select the key size for self-enrolled certificates (1024, 2048, or 4096 bits)
Enable self-enrollment for Smart Card certificate	Select to enable self-enrollment for smart card certificates. This requires that a DNS domain name be configured, as it is used in the CRL Distribution Points certificate extension.

Select *OK* to apply any changes you have made.

Non-compliant devices

802.1X methods require interactive entry of user credentials to prove a user's identity before allowing them access to the network. This is not possible for non-interactive devices, such as printers. MAC Authentication Bypass is supported to allow non-802.1X compliant devices to be identified and accepted onto the network using their MAC address as authentication.

To configure MAC-based authentication for a device:

1. Go to *Authentication* > *User Management* > *MAC Devices*. The MAC device list will be shown.
2. If you are adding a new device, select *Create New* to open the *Create New MAC-based Authentication Device* window.

   If you are editing an already existing device, select the device from the device list.
3. Enter the device name in the *Name* field, and enter the device's MAC address in the *MAC address* field.

Select *OK* to apply your changes.

Fortinet Single Sign-On

FSSO is a set of methods to transparently authenticate users to FortiGate and FortiCache devices. This means that the FortiAuthenticator unit is trusting the implicit authentication of a different system, and using that to identify the user. FortiAuthenticator takes this framework and enhances it with several authentication methods:

- Users can authenticate through a web portal and a set of embeddable widgets.
- Users with FortiClient Endpoint Security installed can be automatically authenticated through the FortiClient SSO Mobility Agent.
- Users authenticating against Active Directory can be automatically authenticated.
- RADIUS Accounting packets can be used to trigger an FSSO authentication.
- Users can be identified through the FortiAuthenticator API. This is useful for integration with third party systems.

This section describes FSSO only. For FSSO authentication methods, there is no need to configure anything in the accounting proxy section.

The FortiAuthenticator unit must be configured to collect the relevant user logon data. After this basic configuration is complete, the various methods of collecting the login information can be set up as needed.

General settings

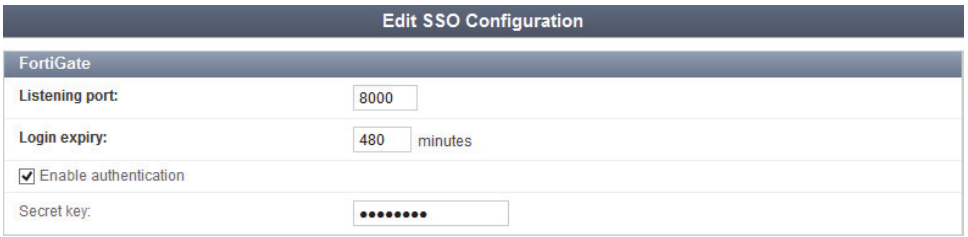
The FortiAuthenticator unit listens for requests from authentication clients and can poll Windows Active Directory servers.

To configure FortiAuthenticator FSSO polling:

1. Go to *Fortinet SSO Methods* > *SSO* > *General* to open the *Edit SSO Configuration* window.

   The *Edit SSO Configuration* window contains sections for FortiGate, FSSO, and user group membership.

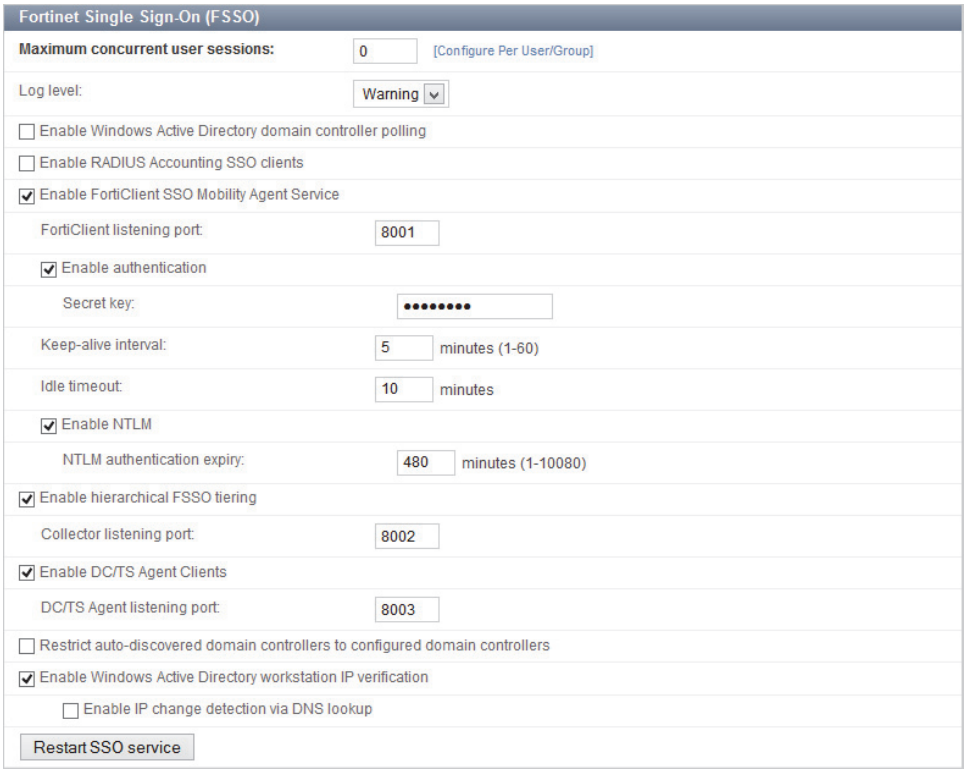
   Figure 82:SSO configuration - FortiGate



2. In the *FortiGate* section, configure the following settings:

Listening port	Leave at 8000 unless your network requires you to change this. Ensure this port is allowed through the firewall.
Login Expiry	The length of time, in minutes, that users can remain logged in before the system logs them off automatically. The default is 480 minutes (8 hours).
Enable authentication	Select to enable authentication, then enter a secret key, or password, in the *Secret key* field.

Figure 83:SSO configuration - FSSO

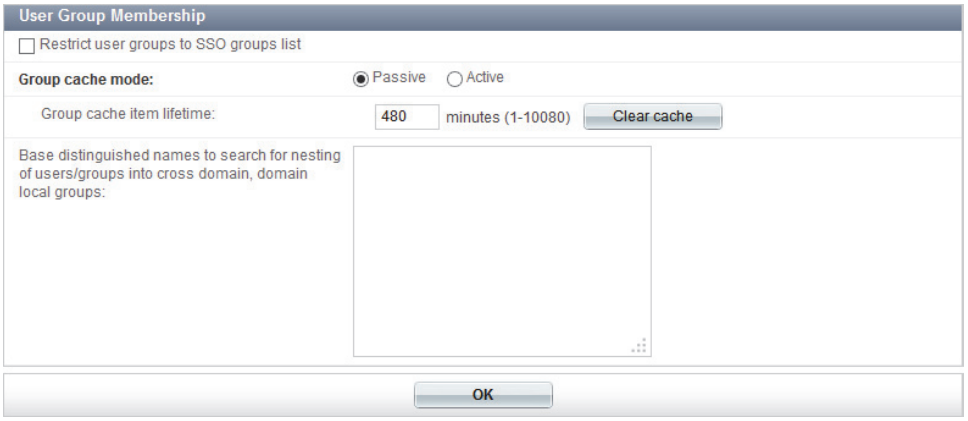


3. In the *Fortinet Single Sign-On (FSSO)* section, enter

Maximum concurrent user sessions	Enter the maximum number of concurrent FSSO login sessions a user is allowed to have. Use *0* for unlimited. Select *Configure Per User/Group* to configure the maximum number of concurrent sessions for each user or group. See "Fine-grained controls" on page 117.
Log Level	Select one of *Debug*, *Info*, *Warning*, or *Error* as the minimum severity level of events to log from the drop-down list.
Enable Windows Active Directory domain controller polling	Select to enable Windows Active Directory polling.
Enable Radius Accounting SSO clients	Select to enable the detection of users sign-ons and sign-offs from incoming RADIUS accounting (Start, Stop, and Interim-Update) records.

Enable FortiClient SSO Mobility Agent Service	Select to enable single sign-on by clients running FortiClient Endpoint Security.
FortiClient listening port	Enter the FortiClient listening port number.
Enable authentication Secret key	Select to enable authentication, then enter a secret key, or password, in the *Secret key* field.
Keep-alive interval	Enter the duration between keep-alive transmissions, from 1 to 60 minutes. Default is 5 minutes.
Idle timeout	Enter an amount of time after which to logoff a user if their status is not updated. The value cannot be lower than the *Keep-alive interval* value.
Enable NTLM	Select to enable the NT LAN Manager (NTLM) to allow logon of users who are connected to a domain that does not have the FSSO DC Agent installed. Disable NTLM authentication only if your network does not support NTLM authentication for security or other reasons. Enter an amount of time after which NTLM authentication expires in the *NTLM authentication expiry* field, from 1 to 10080 minutes (7 days).
Enable hierarchical FSSO tiering	Select to enable hierarchical FSSO tiering. Enter the collector listening port in the *Collector listening port* field.
Enable DC/TS Agent Clients	Select to enable clients using DC or TS Agent. Enter the UDP port in the *DC/TS Agent listening port* field. Default is 8002.
Restrict auto-discovered domain controllers to configured domain controllers	Select to enable restricting automatically discovered domain controllers to already configured domain controllers only. See "Domain controllers" on page 119.
Enable Windows Active Directory workstation IP verification	Select to enable workstation IP verification with Windows Active Directory. If enabled, *select Enable IP change detection via DNS lookup* to detect IP changes via DNS lookup.
Restart SSO service	Select to restart the SSO service.

Figure 84:SSO configuration - user group membership



4. In the *User Group Membership* section, enter

Restrict user groups to SSO groups list	Select to restrict user groups to only those groups in the SSO group list.
Group cache mode	Select the group cache mode: • *Passive*: Items have an expiry time after which the are removed and re-queried on the next logon. • *Active*: Items are periodically updated for all currently logged on users.
Group cache item lifetime	Enter the amount of time after which items will expire. This is only available when the group cache mode is set to passive.
Group cache update period for active logons	Enter the amount of time after which items are updated. This is only available when the group cache mode is set to active.
Base distinguished names to search	Enter the base distinguished names to search for nesting of users or groups into cross domain and domain local groups.

5. Select *OK* to apply the settings.

Configuring FortiGate units for FSSO

Each FortiGate unit that will use FortiAuthenticator to provide Single Sign-On authentication must be configured to use the FortiAuthenticator unit as an SSO server.

To configure Single Sign-On authentication on the FortiGate unit:

1. On the FortiGate unit, go to *User & Device* > *Authentication* > *Single Sign-On* and select *Create New*.
2. In the *Type* field, select *Fortinet Single-Sign-On Agent*.
3. Enter a name for the FortiAuthenticator unit in the *Name* field.
4. In the *Primary Agent IP/Name* field, enter the IP address of the FortiAuthenticator unit.
5. In the *Password* field, enter the secret key that you defined for the FortiAuthenticator unit.
   See “Enable authentication” on page 113.
6. Select OK.

In a few minutes, the FortiGate unit receives a list of user groups from the FortiAuthenticator unit. When you open the server, you can see the list of groups. The groups can be used in identity-based security policies.

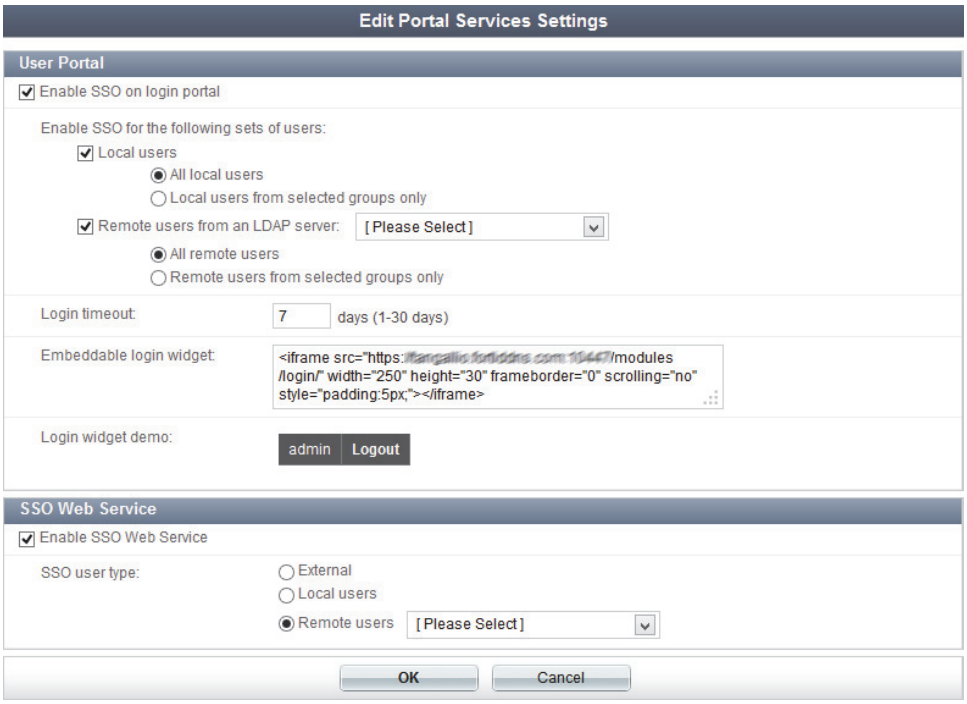
Portal services

The SSO portal supports a logon widget that you can embed in any web page. Typically, an organization would embed the widget on its home page.

The SSO portal sets a cookie on the user's browser. When the user browses to a page containing the login widget, the FortiAuthenticator unit recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login timeout expires, which can be up to 30 days. To log out of FSSO immediately, the user can select the Logout button in the widget.

To configure portal services, go to *Fortinet SSO Methods* > *SSO* > *Portal Services*.

Figure 85: Portal services



In the *User Portal* section, select *Enable SSO login portal* to enable the SSO login portal. In the *SSO Web Service* section, select *Enable SSO Web Service* to use the web service to log users in and out.

The following settings can be configured:

Enable SSO for the following sets of users	
Local users	Select to enable SSO for either all local users or local users from specific groups. If selecting the latter, select the specific groups from the available local user groups.
Remote users from an LDAP server	Select to enable SSO for remote users. Select the LDAP server from the drop-down list, and select either all remote users or remote users from the groups that you select.

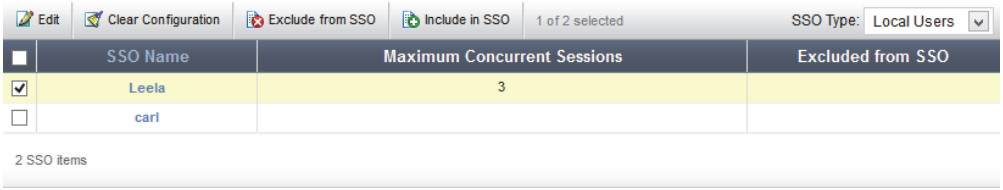
Login timeout	Set the maximum number of days a user is allowed to stay logged in before being logged out automatically from SSO, from 1 to 30 days. Default of 7 days.
Embeddable login widget	Use this code to embed the login widget onto your site. The code cannot be edited manually in this field.
Login widget demo	A demo of what the login widget will look like on your site.
SSO user type	Specify the type of user that the client will provide: external, local, or remote (LDAP server must be selected from the drop-down list).

Fine-grained controls

The *Fine-grained Controls* menu provide options to include or exclude a user or group from SSO, and set the maximum number of concurrent sessions that a user or group can have.

To adjust the controls, go to Fortinet *SSO Methods* > *SSO* > *Fine-grained Controls*.

Figure 86: Fine-grained controls



The following options are available:

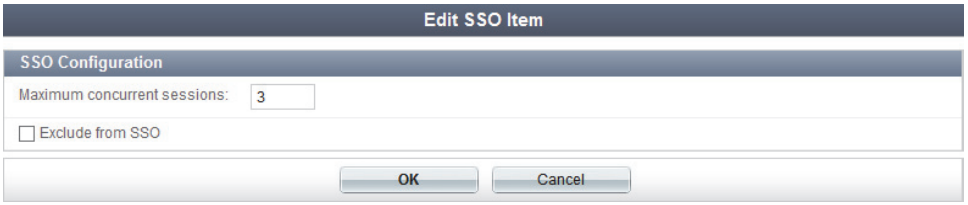
Edit	Edit the selected user's or group's settings. See "To edit an SSO user or group:" on page 118.
Clear Configuration	Clear the SSO configuration for the selected users or groups.
Exclude from SSO	Select a user or users, then select *Exclude from SSO* to exclude them from SSO.
Include in SSO	Select a user or users, then select *Include in SSO* to include the selected users in SSO.
SSO Type	Select the SSO type to view from the drop-down list. The options are: *Local Users*, *Local Groups*, *SSO Users*, and *SSO Groups*.
SSO Name	The users' or groups' names. Select the column title to sort the list by this column.
Maximum Concurrent Sessions	The maximum concurrent sessions allowed for the user or group. This number cannot be greater than five.
Excluded from SSO	If the user or group is excluded from SSO, a red circle with a line will be displayed.

To edit an SSO user or group:

1. In the *Fine-grained Controls* window, select the SSO user or group that is being edited then select *Edit*.

   The *Edit SSO Item* window opens.

   Figure 87: Edit SSO item

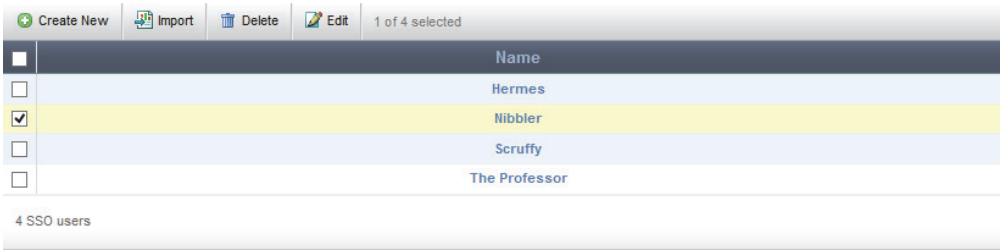


2. Enter the maximum number of concurrent SSO logon sessions per user that the user or group is allowed to have. Enter *0* for unlimited. The number must be equal to or less than five.
3. If the SSO item is a user, select Exclude from SSO to exclude the user from SSO.
4. Select *OK* to apply the changes.

SSO users and groups

To manage SSO users and groups, go to *Fortinet SSO Methods* > *SSO* > *SSO Users* or *Fortinet SSO Methods* > *SSO* > *SSO Groups*.

Figure 88:SSO users



The following options are available:

Create New	Select to create a new user or group. In the *Create New SSO User* or *Create New SSO Group* window, enter a name for the user or group, then select *OK*.
Import	Import SSO users or groups from a remote LDAP server. See "To import SSO users or groups:" on page 119.
Delete	Delete the selected users or groups.
Edit	Edit the selected user or group.
Name	The SSO user or group names.

FortiAuthenticator SSO user groups cannot be used directly in a security policy on a FortiGate device. An FSSO user group must be created on the FortiGate unit, then the FortiAuthenticator SSO groups must be added to it. FortiGate FSSO user groups are available for selection in identity-based security policies. See the *FortiOS Handbook* for more information.

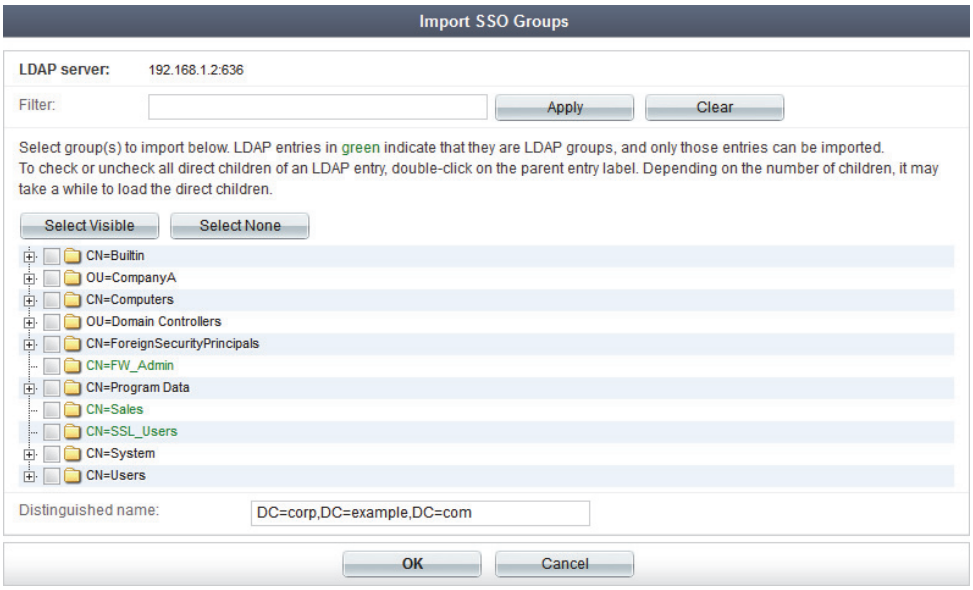
To import SSO users or groups:

1. In the *SSO Users* or *SSO Groups* list, select *Import*.
2. In the *Import SSO Users* or *Import SSO Groups* window, select a remote LDAP server from the *Remote LDAP Server* drop-down list, then select *Import Users* or *Import Groups*.

An LDAP server must already be configured to select it in the drop-down list. See "Remote LDAP servers" on page 95 for information on adding a remote LDAP server.

The *Import SSO Users* or *Import SSO Groups* window opens in a new browser window.

Figure 89: Import SSO groups



3. Optionally, enter a *Filter* string to reduce the number of entries returned, and then select *Apply*, or select *Clear* to clear the filters.
4. Select the entries you want to import and then select *OK*.

Domain controllers

If Active Directory will be used to ascertain group information, the FortiAuthenticator unit must be configured to communicate with the domain controller.

A domain controller entry can be disabled without deleting its configuration. This can be useful when performing testing and troubleshooting, or when moving controllers within your network.

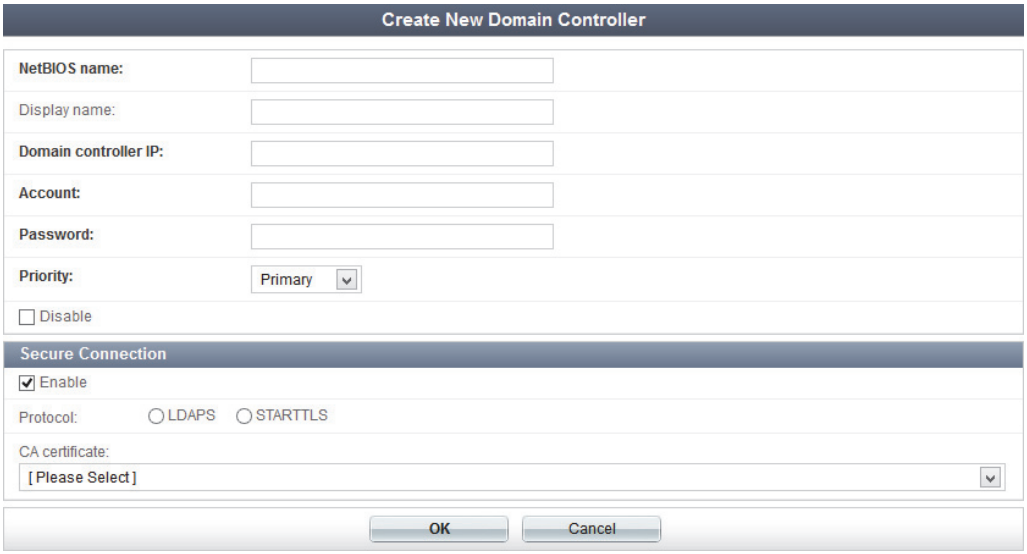
In order to properly discover the available domains and domain controllers, the DNS settings must specify a DNS server that can provide the IP addresses of the domain controllers. See "DNS" on page 44.

To add a domain controller:

1. Go to *Fortinet SSO Methods* > *SSO* > *Domain Controllers*.

2. Select *Create New* to open the *Create New Domain Controller* window.

Figure 90: New domain controller



3. Enter the following information:

NetBIOS Name	Enter the name of the Domain Controller as it appears in NetBIOS.
Display Name	This is a unique name to easily identify this Domain Controller.
Network Address	Enter the network IPv4 address of the controller.
Account	Enter the account name used to access logon events. This account should have administrator rights.
Password	Enter the password for the above account.
Priority	You can define two (or more) Domain Controllers for the same domain. Each can be designated *Primary* or *Secondary*. The *Primary* unit is accessed first.
Disable	Disable the domain controller without losing any of its settings.
Secure Connection	
Enable	*Enable secure connection.*
Protocol	Select a secure connection protocol, either *LDAPS* or *STARTTLS*.
CA certificate	Select a certificate from the drop-down list.

4. Select OK.

By default, FortiAuthenticator uses auto-discovery of Domain Controllers. If you want to restrict operation to the configured domain controllers only, go to *Fortinet SSO Methods* > *SSO* > *General* and select *Restrict auto-discovered domain controllers to configured domain controllers*. See “General settings” on page 112.

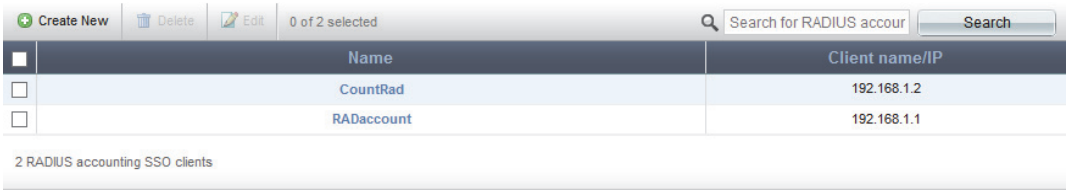
RADIUS accounting

If required, SSO can be based on RADIUS accounting records. The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server or network device, such as a wireless controller, collects additional group information, and then inserts it into FSSO to be used by multiple FortiGate or FortiCache devices for identity based policies.

The FortiAuthenticator must be configured as a RADIUS accounting client to the RADIUS server.

To view the RADIUS accounting SSO client list, go to *Fortinet SSO Methods* > *SSO* > *RADIUS Accounting*.

Figure 91:RADIUS accounting SSO client list

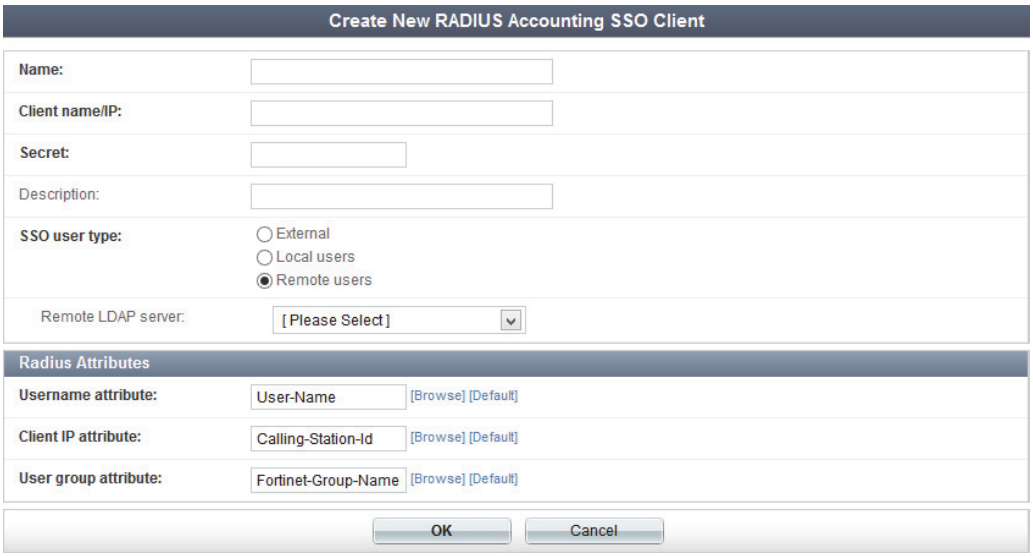


To configure and enable a RADIUS accounting client:

1. From the RADIUS accounting SSO client list, select *Create New*.

   The *Create New RADIUS Accounting SSO Client* window opens.

   Figure 92: New RADIUS accounting SSO client



2. Enter the following information:

Name	Enter a name in the *Name* field to identify the RADIUS accounting client on the FortiAuthenticator.
Client name/IP	Enter the RADIUS accounting client's FQDN or IP address.
Secret	Enter the RADIUS accounting client's preshared key.
Description	Optionally, enter a description of the client.

SSO user type	Specify the type of user that the client will provide: external, local, ore remote (LDAP server must be selected from the drop-down list).
Radius Attributes	If required, customize the username, client IP, and user group RADIUS attributes to match the ones used in the incoming RADIUS accounting records. See "RADIUS attributes" on page 85.

3. Select *OK* to apply the changes.
4. Enable RADIUS accounting SSO clients by going to *Fortinet SSO Methods* > *SSO* > *General* and selecting *Enable RADIUS Accounting SSO clients*. See "General settings" on page 112.

FortiGate group filtering

If you are providing SSO to only certain groups on a remote LDAP server, you can filter the polling information so that it includes only those groups.

To view a list of the FortiGate group filters, go to *Fortinet SSO Methods* > *SSO* > *FortiGate Group Filtering.*

To create a new group filter:

1. From the FortiGate group filters select *Create New*.

   The *Create New FortiGate Group Filter* window opens.

Figure 93: New FortiGate group filter

2. Enter the following information:

Name	Enter a name in the *Name* field to identify the filter.
FortiGate name/IP	Enter the FortiGate unit's FQDN or IP address.
Description	Optionally, enter a description of the filter.
Forward FSSO information for users from the following subset of groups only	Select to forward SSO information for users from only the specific subset of groups. Choose the desired SSO groups from the *Available sso groups* box and move them to the *Selected sso groups* box. See "SSO users and groups" on page 118 for information on SSO groups.
Enable IP filtering for this service	Select to enable IP filtering for this service. Choose the desired IP filtering rules from the *Available IP filtering rules* box and move them to the *Selected IP filtering rules* box. See "IP filtering rules" on page 123 for more information.

3. Select *OK* to create the new FortiGate group filter.

IP filtering rules

The user logon information that is sent to the FortiGate units can be restricted to specific IP addresses or address ranges. If no filters are defined, information is sent for all addresses.

To view a list of the IP filtering rules, go to *Fortinet SSO Methods* > *SSO* > *IP Filtering Rules*.

To create new IP filtering rules:

1. From the IP filtering rules list, select *Create New*.
   The *Create New IP Filtering Rule* window opens.

Figure 94: New IP filtering rule

2. Enter the following information:

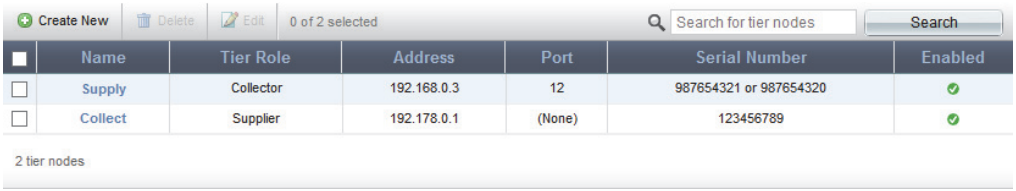
Name	Enter a name for the rule.
Filter Type	Select whether the rule will specify an IP address and netmask or an IP address range.
Rule	Enter wither an IP address and netmask or an IP address range (depending on the selected filter type). For example: • IP/Mask: `10.0.0.1/255.255.255.0` • IP Range: `10.0.0.1/10.0.0.99`

3. Select *OK* to create the new IP filtering rule.

Tiered architecture

Tier nodes can be managed by going to *Fortinet SSO Methods* > *SSO* > *Tiered Architecture*.

Figure 95: Tier nodes



The following options are available:

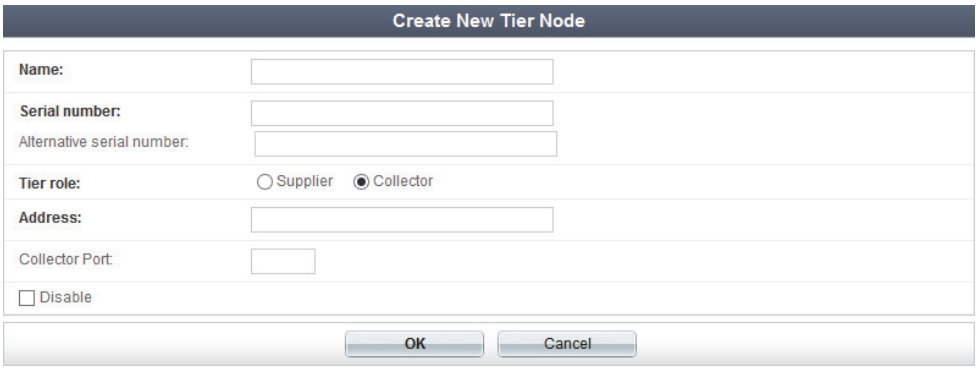
Create New	Select to create a new tier node. See "To add a new tier node:" on page 124.
Delete	Select to delete the selected node or nodes.
Edit	Select to edit the selected node.
Search	Enter a search term in the search text box then select *Search* to search the tier node list.
Name	The node name.
Tier Role	The node's tier role, either *Collector* or *Supplier*.
Address	The IP address of the node.
Port	The collector port number. Only applicable if *Tier Role* is *Collector*.
Serial Number	The serial number or numbers.
Enabled	If the node is enabled, a green circle with a check mark will be shown. A node can be disabled without losing any of its settings.

To add a new tier node:

1. From the tier node list, select *Create New*.

   The *Create New Tier Node* window opens.

   Figure 96: New tier node



2. Enter the following information:

Name	Enter a name to identify the node.
Serial number	Enter the device serial number.
Alternate serial number	Optionally, enter a second, or alternate, serial number for an HA cluster member.
Tier Role	Select the tier node role, either *Supplier* or *Collector*.
Address	Enter the IP address for the supplier or collector.

Collector port	Enter the collector port number. Default is 8002. This only applies is *Collector* is selected as the *Tier Role*.
Disable	Disable the node without losing any of its settings.

3. Select *OK* to create the new tier node.

FortiClient SSO Mobility Agent

The FortiClient SSO Mobility Agent is a feature of FortiClient Endpoint Security. The agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The *FortiClient SSO Mobility Agent Service* must be enabled. See "Enable FortiClient SSO Mobility Agent Service" on page 114.

For information on configuring FortiClient, see the *FortiClient Administration Guide* for your device.

Fake client protection

Some attacks are based on a user authenticating to an unauthorized AD server in order to spoof a legitimate user logon through the FortiClient SSO Mobility Agent. You can prevent this type of attack by enabling NTLM authentication (see "Enable NTLM" on page 114).

The FortiAuthenticator unit will initiate NTLM authentication with the client, proxying the communications only to the legitimate AD servers it is configured to use.

If NTLM is enabled, the FortiAuthenticator unit requires NTLM authentication when:

- the user logs on to a workstation for the first time,
- the user logs off and then logs on again,
- the workstation IP address changes,
- the workstation user changes,
- NTLM authentication expires (user configurable).

RADIUS Single Sign-On

A FortiGate or FortiMail unit can transparently identify users who have already authenticated on an external RADIUS server by parsing RADIUS accounting records. However, this approach has potential difficulties:

- The RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.
- In some cases, the server can send accounting records only to a single endpoint. Some network topologies may require multiple endpoints.

The FortiAuthenticator RADIUS Accounting Proxy overcomes these limitations by proxying the RADIUS accounting records, modifying them, and replicating them to the multiple subscribing endpoints as needed.

RADIUS accounting proxy

The FortiAuthenticator receives RADIUS accounting packets from a carrier RADIUS server, transforms them, and then forwards them to multiple FortiGate or FortiMail devices for use in RADIUS Single Sign-On. This differs from the packet use of RADIUS accounting ("RADIUS accounting" on page 121).

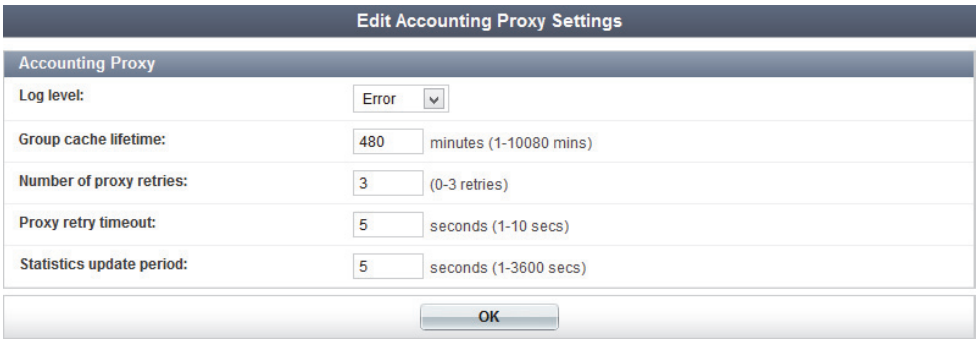
The accounting proxy needs to know:

- Rule sets to define or derive the RADIUS attributes that the FortiGate unit requires,
- The source of the RADIUS accounting records: the RADIUS server,
- The destination(s) of the accounting records: the FortiGate units using this information for RADIUS SSO authentication.

General settings

General RADIUS accounting proxy settings can be configure by going to *Fortinet SSO Methods* > *Accounting Proxy* > *General*.

Figure 97: General accounting proxy settings



The following settings are available:

Log level	Select one of *Debug*, *Info*, *Warning*, or *Error* as the minimum severity level of event to log from the drop-down list.
Group cache lifetime	Enter the amount of time after which user group memberships will expire in the cache, from 1 to 10080 minutes (7 days). The default is 480 minutes.
Number of proxy retries	Enter the number of times to retry proxy requests if they timeout, from 0 to 3 retries, where 0 disables retries. The default is 3 retries.
Proxy retry timeout	Enter the retry period (timeout) of a proxy request, from 1 to 10 seconds.
Statistics update period	Enter the time between statistics updates to the seconds debug log, from 1 to 3600 seconds (1 hour).

Select *OK* to apply your changes.

Rule sets

A rule set can contain multiple rules. Each rule can do one of:

- add an attribute with a fixed value
- add an attribute retrieved from a user's record on an LDAP server
- rename an attribute to make it acceptable to the accounting proxy destination.

The FortiAuthenticator unit can store up to 10 rule sets. You can provide both a name and a description to each rule set to help you remember each rule set's purpose.

Rules access RADIUS attributes of which there are both standard attributes and vendor-specific attributes (VSAs). To select a standard attribute, select the Default vendor. See "RADIUS attributes" on page 85.

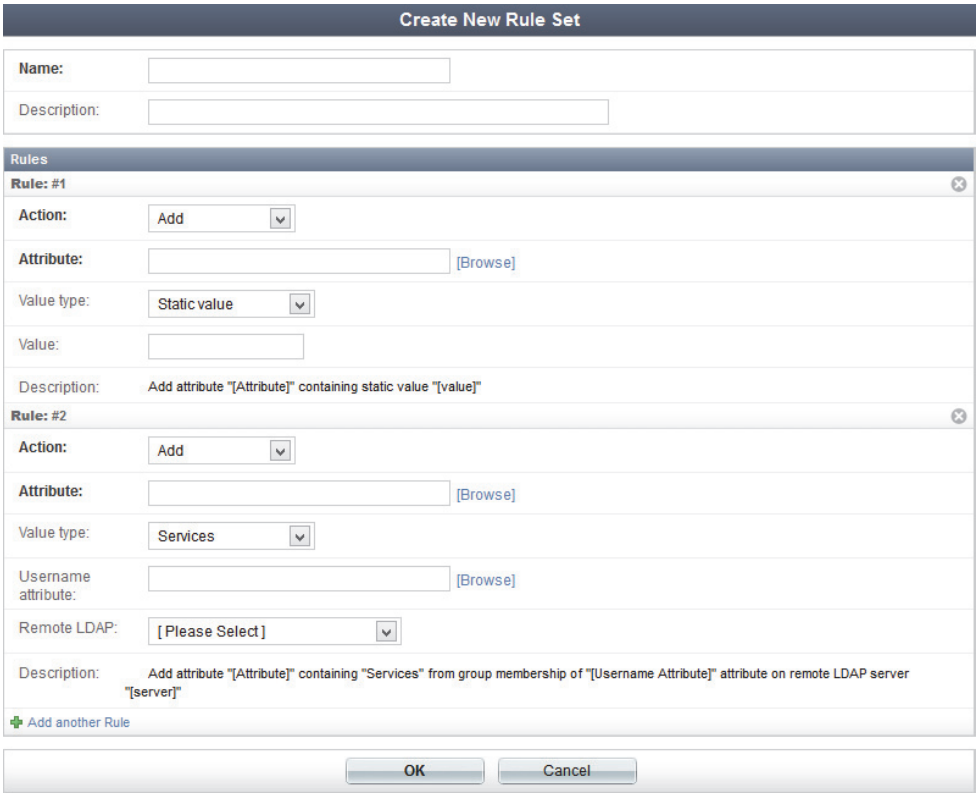
To view the accounting proxy rule set list, go to *Fortinet SSO Methods* > *Accounting Proxy* > *Rule Sets*.

To add RADIUS accounting proxy rule sets:

1. From the rule set list, select *Create New*.

   The *Create New Rule Set* window opens.

Figure 98: New RADIUS accounting proxy rule set



2. Enter the following information:

Name	Enter a name to use when selecting this rule set for an accounting proxy destination.
Description	Optionally, enter a brief description of the rule's purpose.
Rules	Enter one or more rules.
Action	The action for each rule can be either *Add* or *Modify*. • *Add*: add either a static value or a value derived from an LDAP server. • *Modify*: rename an attribute.
Attribute	Select *Browse* and choose the appropriate Vendor and Attribute ID in the *Select a RADIUS Attribute* dialog box.
Attribute 2	If the action is set to *Modify*, a second attribute may be selected. The first attribute will be renamed to the second attribute.

Value Type	If the action is set to *Add*, select a value type from the drop-down list. • *Static value*: adds the attribute in the *Attribute* field containing the static value in the *Value* field. • *Group names*: adds attribute in the *Attribute* field containing "Group names" from the group membership of the *Username Attribute* on the remote LDAP server. • *Services*: adds attribute in the *Attribute* field containing "Services" from the group membership of the *Username Attribute* on the remote LDAP server. • *UTM profile groups*: adds attribute in the *Attribute* field containing "UTM profile groups" from the group membership of the *Username Attribute* on the remote LDAP server.
Value	If the action is set to *Add* and *Value Type* is set to *Static value*, enter the static value.
Username Attribute	If the action is set to *Add,* and *Value Type* is not set to *Static value*, specify an attribute that provides the user's name.
Remote LDAP	If the attribute addition requires an LDAP server, select one that has been defined in *Authentication* > *Remote Auth. Servers* from the drop-down list. See "Remote LDAP servers" on page 95
Description	A brief description of the rule is provided.
Add another rule	Select to add another rule to the rule set.

3. Select *OK* to create the new rule set.

Example rule set

The incoming accounting packets contain the following fields:

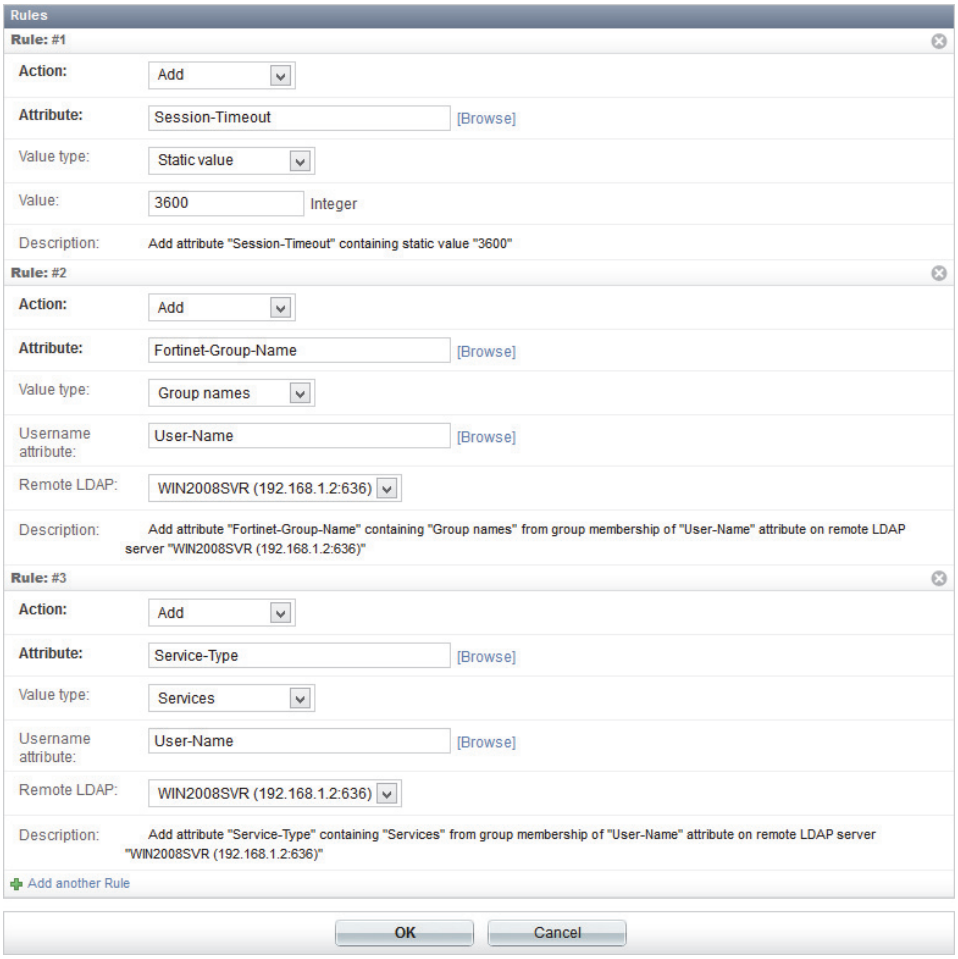
- User-Name
- NAS-IP-Address
- Fortinet-Client-IP-Address

The outgoing accounting packets need to have these fields:

- User-Name
- NAS-IP-Address
- Fortinet-Client-IP-Address
- Session-Timeout: Value is always 3600
- Fortinet-Group-Name: Value is obtained from user's group membership on remote LDAP
- Service-Type: Value is obtained from user's group membership and SSO Group Mapping

The rule set needs three rules to add Session-Timeout, Fortinet-Group-Name, and Service-Type.

Figure 99: Example rule set



Sources

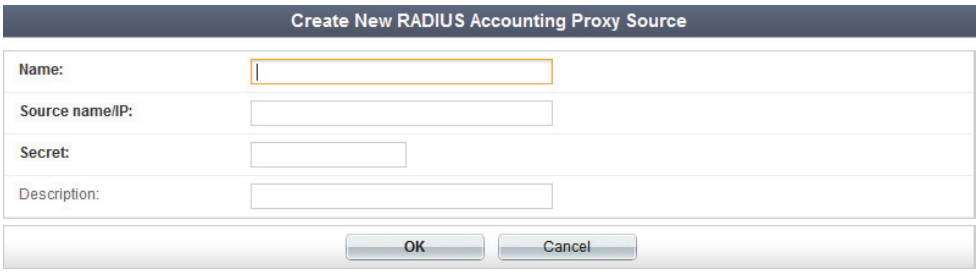
The RADIUS accounting proxy sources list can be viewed in *Fortinet SSO Methods* > *Accounting Proxy* > *Sources*. Sources can be added, edited, and deleted as needed.

To add a RADIUS accounting proxy source:

1. From the source list, select *Create New*.

   The *Create New RADIUS Accounting Proxy Source* window opens.

   Figure 100: New RADIUS accounting proxy source



2. Enter the following information:

Name	Enter the name of the RADIUS server. This is used in FortiAuthenticator configurations.
Source name/IP	Enter the FQDN or IP address of the server.
Secret	Enter the shared secret required to access the server.
Description	Optionally, enter a description of the source.

3. Select *OK* to add the RADIUS accounting proxy source.

Destinations

The destination of the RADIUS accounting records is the FortiGate unit that will use the records to identify users. When defining the destination, you also specify the source of the records (a RADIUS client already defined as a source) and the rule set to apply to the records.

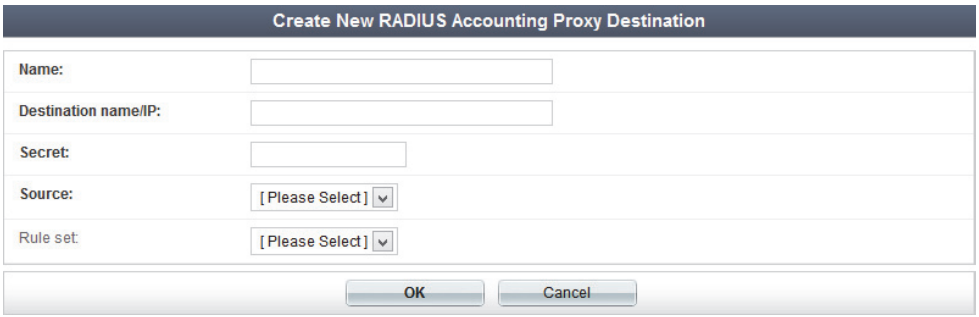
To view the RADIUS accounting proxy destinations list, go to *Fortinet SSO Methods* > *Accounting Proxy* > *Destinations*.

To add a RADIUS accounting proxy destinations:

1. From the destinations list, select *Create New*.

   The *Create New RADIUS Accounting Proxy Destination* window opens.

   Figure 101: New RADIUS accounting proxy destination



2. Enter the following information:

Name	Enter A name to identify the destination device in your configuration.
Destination name/IP	Enter The FQDN or IP address of the FortiGate that will receive the RADIUS accounting records.
Secret	Enter the preshared key of the destination.
Source	Select a RADIUS client defined as a source from the drop-down list. See “Sources” on page 130.
Rule set	Select an appropriate rule set from the drop-down list. See “Rule sets” on page 127.

3. Select *OK* to add the RADIUS accounting proxy destination.

Monitoring

The *Monitor* menu tree provides options for monitoring SSO and authentication activity.

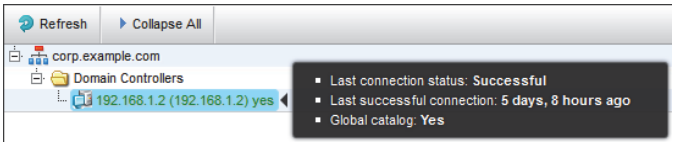
SSO

FortiAuthenticator can monitor the units that make up FSSO. This is useful to ensure there is a connection to the different components when troubleshooting.

Domains

To monitor SSO domains, go to *Monitor* > *SSO* > *Domains*. Select *Refresh* to refresh the domain list. Select *Expand All* to expand all of the listed domains, or *Collapse All* to collapse the view.

Figure 102:SSO domains

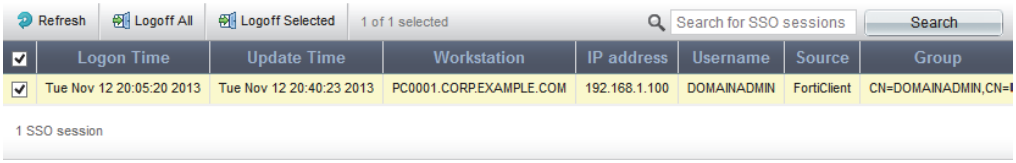


Hover the cursor over an entry to view additional information, such as the status and length of the last connection.

SSO sessions

To monitor SSO sessions, go to *Monitor* > *SSO* > *SSO Sessions*. Users can be manually logged off of if required.

Figure 103:SSO sessions



The following information is available:

Refresh	Refresh the SSO sessions list.
Logoff All	Log off all of the connected users.
Logoff Selected	Log off only the selected users.
Search	Enter a search term in the search field, then select *Search* to search the SSO sessions list.
Logon Time	When the session was started.
Update Time	When the session was last updated.

Workstation	The workstation that the user is using.
IP address	The IP address of the workstation.
Username	The username of the user.
Source	The source of the connection.
Group	The group to which the user belongs.

Domain controllers

Domain controllers that are registered with the FortiAuthenticator unit can be viewed by going to *Monitor* > *SSO* > *Domain Controllers*.

Figure 104:SSO domain controllers

The domain controllers list can be refreshed by selecting *Refresh*, and searched using the search field.

The list shows the connection status of the domain controller, as well as its update time and IP address. The total number of events, as well as the most recent event, are also shown.

FortiGate

FortiGate units that are registered with the FortiAuthenticator unit can be viewed at *Monitor* > *SSO* > *FortiGates*.

Figure 105:SSO FortiGate units

The list can be refreshed by selecting *Refresh*, and searched using the search field. The list shows the connection time of each device, as well as its IP address and serial number.

User authentication events are logged in the FortiGate event log. See the *FortiGate Handbook* for more information.

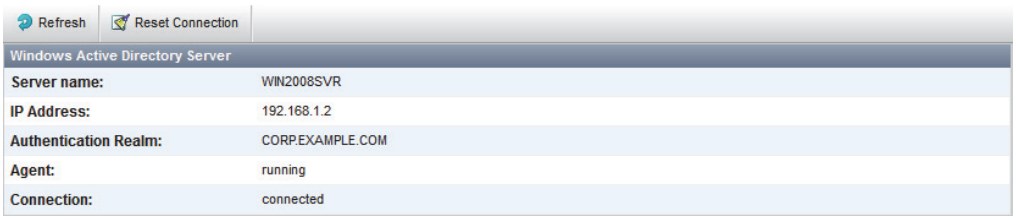
Authentication

The Windows AD server and inactive users can be monitored from *Monitor* > *Authentication*.

Windows AD

To view the Windows AD server information, go to *Monitor* > *Authentication* > *Windows AD*.

Figure 106: Windows AD server information

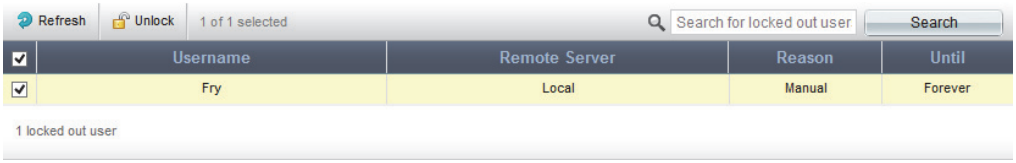


To refresh or reset the connection, select *Refresh* or *Reset Connection* in the toolbar. The server name, IP address, authentication realm, agent, and connection are shown.

Inactive users

To view a list of locked out, or inactive, users, go to *Monitor* > *Authentication* > *Inactive Users*.

Figure 107: Inactive users



To unlock a user from the list, select the user, then select *Unlock*. The list can be refreshed by selecting *Refresh*, and searched using the search field.

The list shows the username, server, the reason the user was locked out, and when they are locked out until.

For more information on locked out users, see “Top User Lockouts widget” on page 41, “Lockouts” on page 67, and “User management” on page 70.

Certificate Management

This section describes managing certificates with the FortiAuthenticator device.

FortiAuthenticator can act as a CA for the creation and signing of X.509 certificates, such as server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPSEC VPN.

The FortiAuthenticator unit has several roles that involve certificates:

Certificate authority	The administrator generates CA certificates that can validate the user certificates generated on this FortiAuthenticator unit. The administrator can import other CA's CA certificates and Certificate Revocation Lists (CRLs), and generate, sign, and revoke user certificates. See "End entities" on page 136 for more information.
SCEP server	A SCEP client can retrieve any of the local CA certificates ("Local CAs" on page 143), and can have its own user certificate signed by the FortiAuthenticator unit CA.
Remote LDAP Authentication	Acting as an LDAP client, the FortiAuthenticator unit authenticates users against an external LDAP server. It verifies the identity of the external LDAP server by using a trusted CA certificate, see "Trusted CAs" on page 151.
EAP Authentication	The FortiAuthenticator unit checks that the client's certificate is signed by one of the configured authorized CA certificates, see "Certificate authorities" on page 143. The client certificate must also match one of the user certificates, see "End entities" on page 136.

Any changes made to certificates generate log entries that can be viewed at *Logging* > *Log Access* > *Logs*. See "Logging" on page 94.

This chapter includes the following sections:

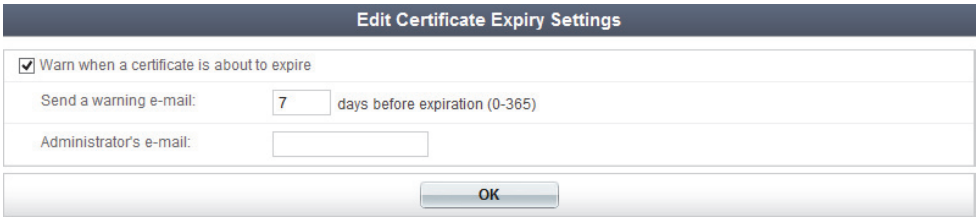
Policies

The policies section includes global configuration settings which are applied across all certificate authorities and end-entity certificates created on the FortiAuthenticator device.

Certificate expiry

Certificate expiration settings can be configured in *Certificate Management* > *Policies* > *Certificate Expiry*.

Figure 108: Edit certificate expiry settings



The following settings can be configured:

Warn when a certificate is about to expire	Enable sending a warning message to an administrator before a certificate expires.
Send a warning e-mail	Enter the number of days before the certificate expires that the email will be sent.
Administrator's e-mail	Enter the email address to which the expiry warning message will be sent.

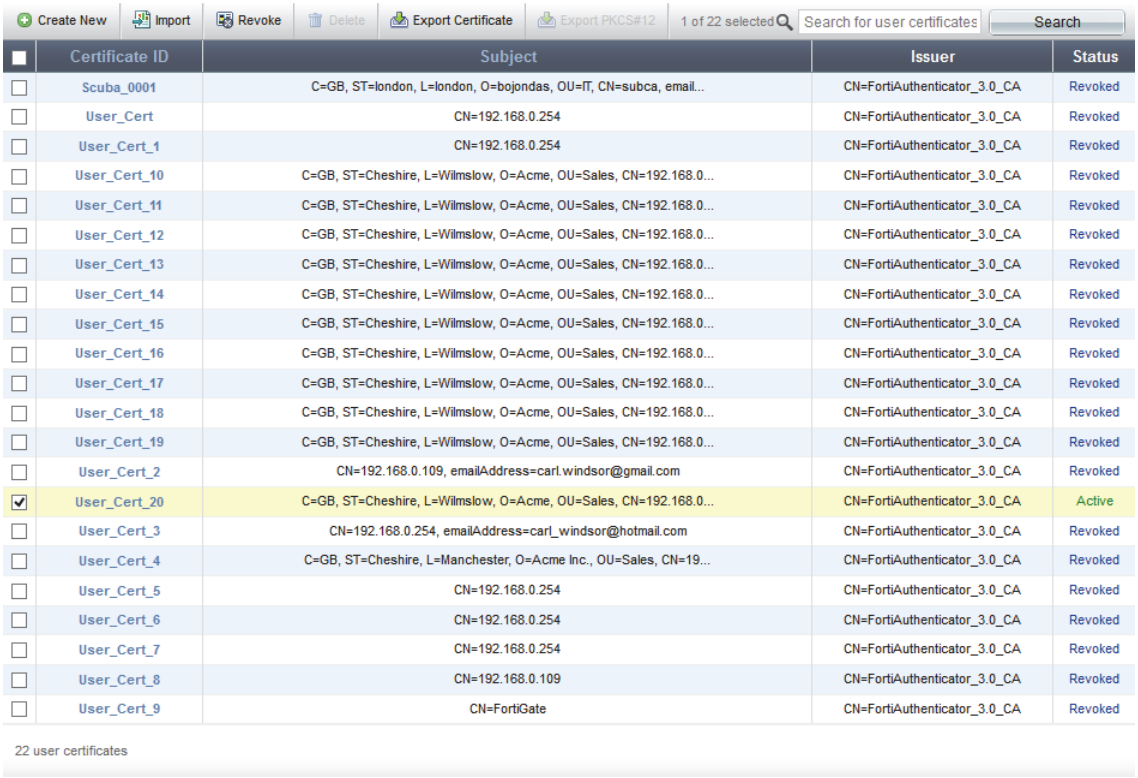
Select *OK* to apply any configuration changes.

End entities

User and server certificates are required for mutual authentication on many HTTPS, SSL, and IPsec VPN network resources. You can create a user certificate on the FortiAuthenticator device, or import and sign a CSR. User certificates, client certificates, or local computer certificates are all the same type of certificate.

To view the user certificate list, go to *Certificate Management* > *End Entities* > *Users*. To view the server certificate list, go to *Certificate Management* > *End Entities* > *Local Services*.

Figure 109: User certificate list



The following information is available:

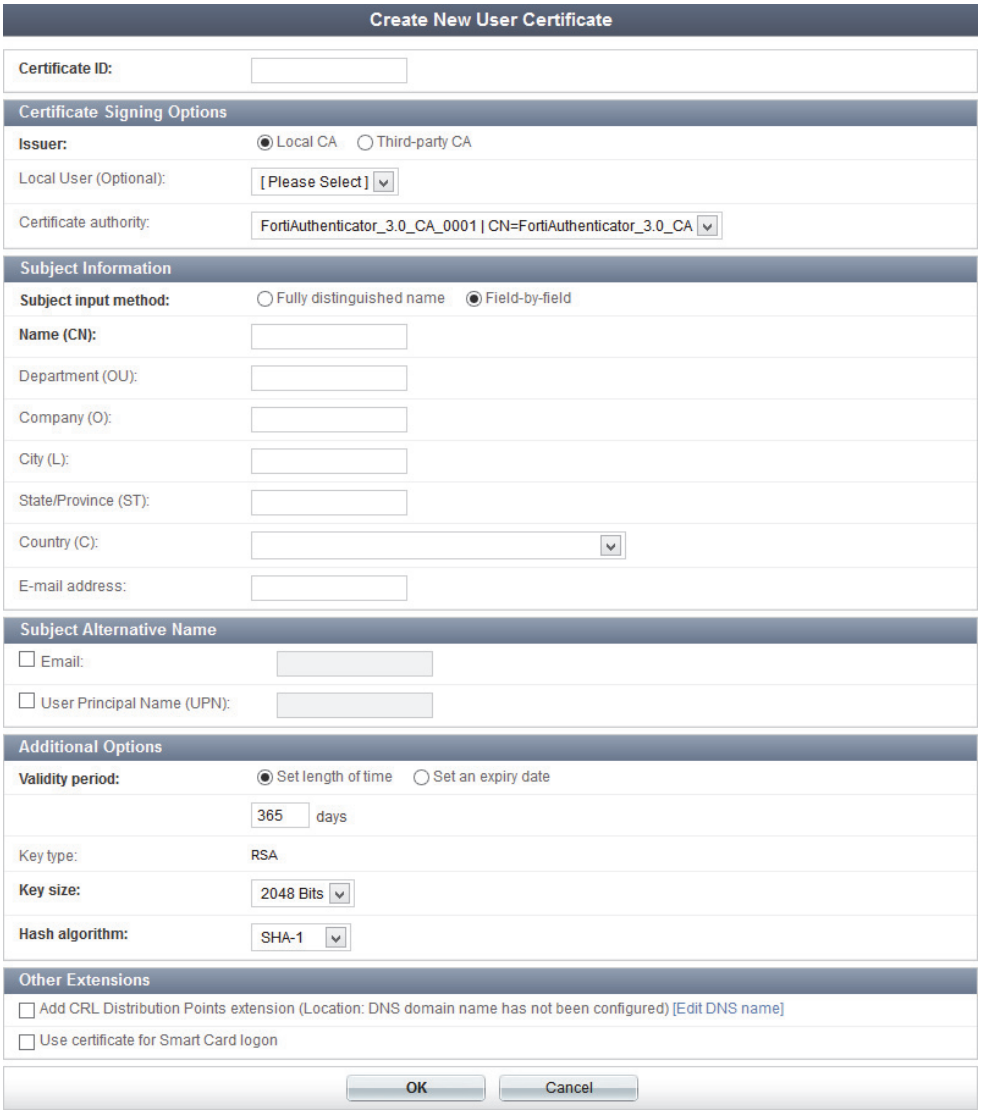
Create New	Create a new certificate. See “To create a new certificate:” on page 138.
Import	Select to import a certificate signed by a third-party CA for a previously generated CSR (see “To import a local user certificate:” on page 140 and “To import a server certificate:” on page 140) or to import a CSR to sign (see “To import a CSR to sign:” on page 141).
Revoke	Revoke the selected certificate. See “To revoke a certificate:” on page 142.
Delete	Delete the selected certificate.
Export Certificate	Save the selected certificate to your computer.
Export PKCS#12	Export the PKCS#12. This is only available for user certificates.
Search	Enter a search term in the search field, then select *Search* to search the certificate list.
Certificate ID	The certificate ID.
Subject	The certificate’s subject.
Issuer	The issuer of the certificate.
Status	The status of the certificate, either active, pending, or revoked.

Certificates can be created, imported, exported, revoked, and deleted as required. CSRs can be imported to sign, and the certificate detail information can also be viewed, see “To view certificate details:” on page 143.

To create a new certificate:

1. To create a new user certificate, go to *Certificate Management* > *End Entities* > *Users*. To create a new server certificate, go to *Certificate Management* > *End Entities* > *Local Services*.
2. Select *Create New* to open the *Create New User Certificate* or *Create New Server Certificate* window.

Figure 110: New user certificate



3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.
Certificate Signing Options	
Issuer	Select the issuer of the certificate, either *Local CA* or *Third-party CA*. Selecting *Third-party CA* generates a CSR that is to be signed by a third-party CA.
Local User	If *Local CA* is selected as the issuer, you may select a local user from the drop-down list to whom the certificate will apply. This option is only available when creating a new user certificate.
Certificate authority	Select one of the available CAs configured on the FortiAuthenticator unit from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See "Certificate authorities" on page 143.
Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Subject DN	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.
Field-by-field	If the subject input method is field-by-field, enter the subject name in the *Name (CN)* field, and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Subject Alternative Name	
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the user principal name used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.

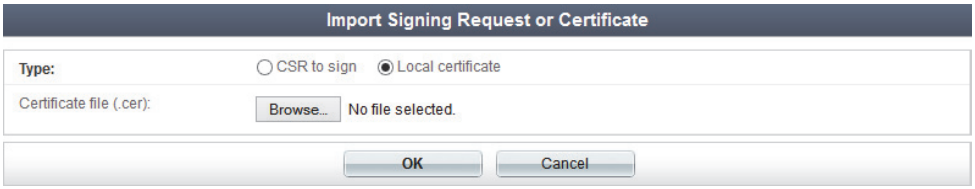
Additional Options	
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Key type	The key type is set to RSA.
Key size	Select the key size from the drop-down list: 1024, 2048, or 4096 bits.
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Other Extensions	This option is only available when creating a new user certificate.
Add CRL Distribution Points extension	Select to add CRL distribution points extension to the certificate. Once a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location. A DNS domain name must be configured. If it has not been, select *Edit DNS name* to configure one. See "DNS" on page 44.
Use certificate for Smart Card logon	Select to use the certificate for smart card logon.

4. Select *OK* to create the new certificate.

To import a local user certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Import*.
2. In the *Import Signing Request or Certificate* window, in the *Type* field, select *Local certificate*.

Figure 111: Import a local user certificate



3. Select *Browse...* to locate the certificate file on your computer.
4. Select *OK* to import the certificate.

To import a server certificate:

1. to *Certificate Management* > *End Entities* > *Local Services* and select *Import*.
2. In the *Import Certificate* window, select *Browse...* to locate the certificate file on your computer.
3. Select *OK* to import the certificate.

To import a CSR to sign:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Import*.
2. In the *Import Signing Request or Certificate* window, in the *Type* field, select *CSR to sign*.

Figure 112: Import a CSR

3. Configure the following settings:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select *Browse...* then locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs configured on the FortiAuthenticator from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See "Certificate authorities" on page 143.
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Subject Alternative Name	
Email	Enter the email address of a user to map to this certificate.

User Principal Name (UPN)	Enter the user principal name used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Other Extensions	
Add CRL Distribution Points extension	Select to add CRL distribution points extension to the certificate. Once a certificate is issued with this extension, the server must be able to handle the CRL request at the specified location. A DNS domain name must be configured. If it has not been, select *Edit DNS name* to configure one. See "DNS" on page 44.
Use certificate for Smart Card logon	Select to use the certificate for smart card logon.

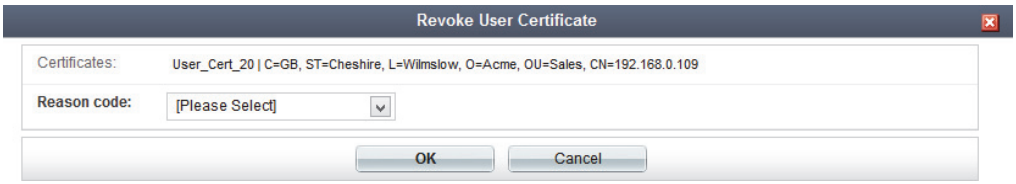
4. Select *OK* to import the CSR.

To revoke a certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* or to *Certificate Management* > *End Entities* > *Local Services*.
2. Select the certificate the will be revoked, then select *Revoke*.

   The *Revoke User Certificate* or *Revoke Server Certificate* window opens.

   Figure 113: Revoke a user certificate



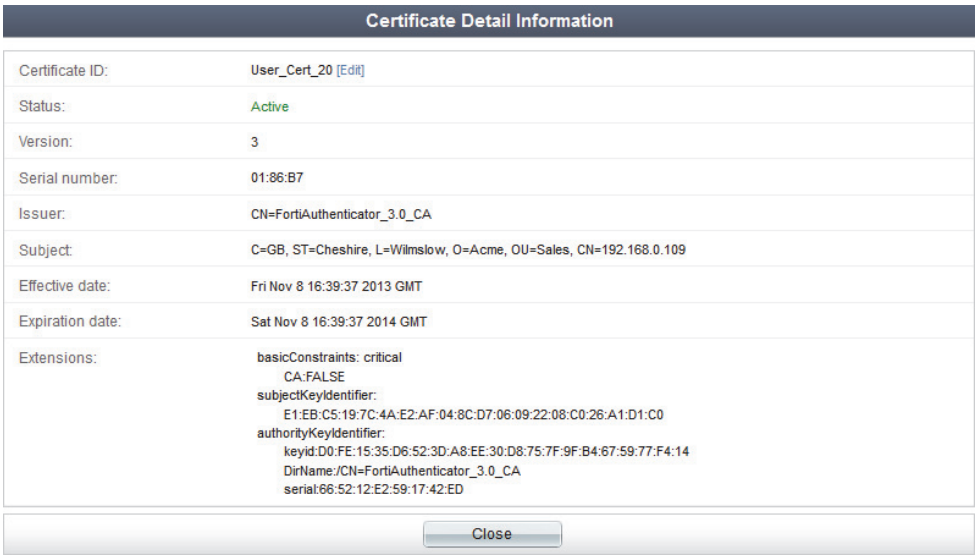
3. Select a reason for revoking the certificate from the *Reason code* drop-down list. The options available are: *Unspecified*, *Key has been compromised*, CA *has been compromised*, *Changes in affiliation*, *Superseded*, *Operation ceased*, and *On Hold*.

   Some of these reasons are security related (such as the key or CA being compromised), while others are more business related; a change in affiliation could be an employee leaving the company; operation ceased could be a project that was cancelled.
4. Select *OK* to revoke the certificate.

To view certificate details:

From the certificate list, select a certificate ID to open the *Certificate Detail Information* window.

Figure 114: Certificate detail information



Select *Edit* next to the Certificate ID field to change the certificate ID. If any of this information is out of date or incorrect, you will not be able to use this certificate.If this is the case, delete the certificate and re-enter the information in a new certificate, see "To create a new certificate:" on page 138. Select *Close* to return to the certificate list.

Certificate authorities

A CA is used to sign other server and client certificates. Different CAs can be used for different domains or certificates. For example, if your organization is international you may have a CA for each country, or smaller organizations might have a different CA for each department. The benefits of multiple CAs include redundancy, in case there are problems with one of the well-known trusted authorities.

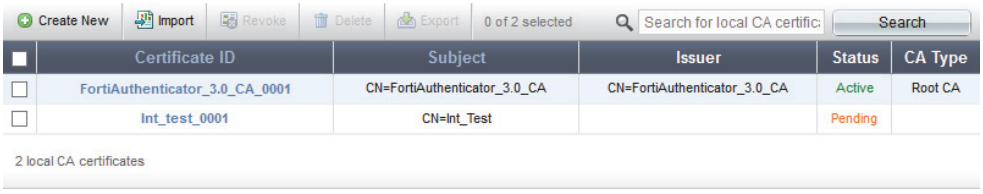
Once you have created a CA certificate, you can export it to your local computer.

Local CAs

The FortiAuthenticator device can act as a self-signed or local CA.

To view the certificate information, go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.

Figure 115: Local CAs list



The following information in shown:

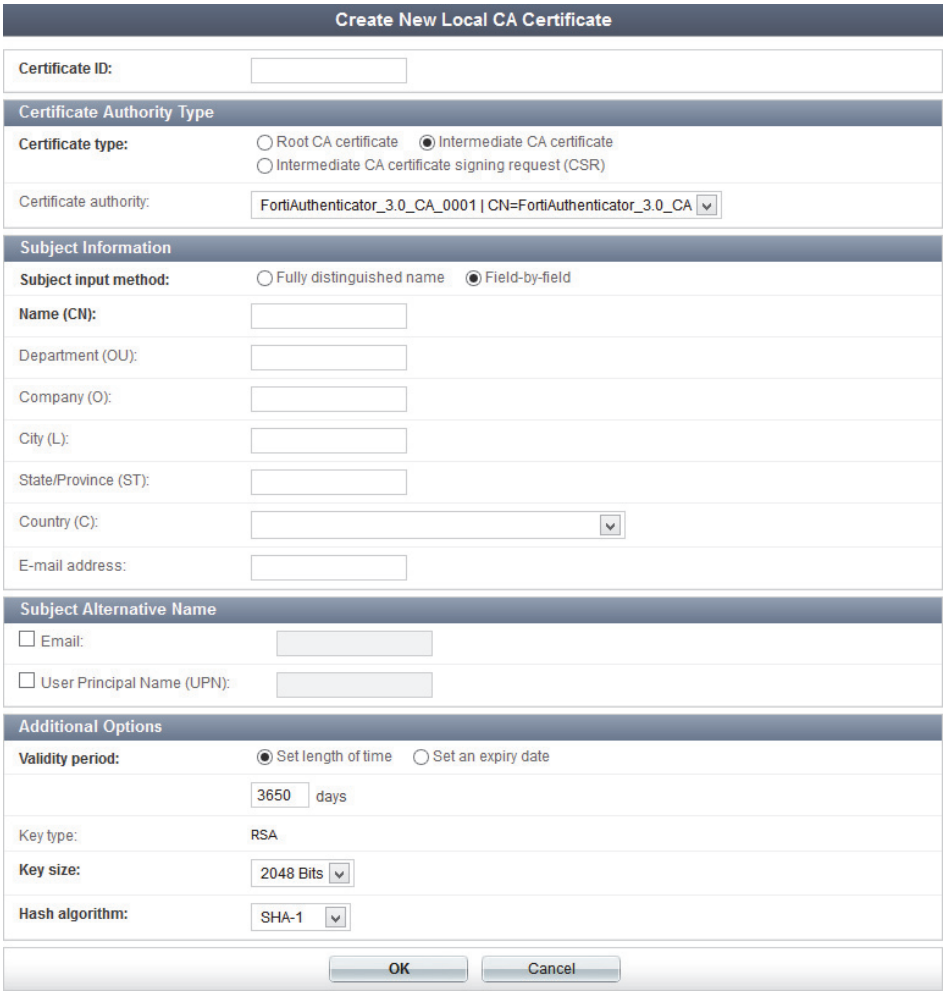
Create New	Create a new CA certificate. See “To create a CA certificate:” on page 145.
Import	Import a CA certificate. See “Importing CA certificates and signing requests” on page 147.
Revoke	Revoke the selected CA certificate. For information on revoking certificates, see “To revoke a certificate:” on page 142.
Delete	Delete the selected CA certificate.
Export	Save the selected CA certificate to your computer.
Search	Enter a search term in the search field, then select *Search* to search the CA certificate list. The search will return certificates that match either the subject or issuer.
Certificate ID	The CA certificate ID.
Subject	The CA certificate subject.
Issuer	The issuer of the CA certificate.
Status	The status of the CA certificate, either active, pending, or revoked.
CA Type	The CA type of the CA certificate.

To create a CA certificate:

1. From the local CA certificate list, select *Create New*.

   The *Create New Local CA Certificate* window opens.

Figure 116: New local CA certificate



2. Enter the following information:

Certificate ID	Enter a unique ID for the CA certificate.
Certificate Authority Type	
Certificate type	Select one of the following options: • *Root CA certificate*: a self-signed CA certificate • *Intermediate CA certificate*: a CA certificate that refers to a different root CA as the authority • *Intermediate CA certificate signing request (CSR)*
Certificate authority	Select one of the available CAs from the drop-down list. This field is only available when the certificate type is *Intermediate CA certificate*.

Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Subject DN	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.
Field-by-field	If the subject input method is field-by-field, enter the subject name in the *Name (CN)* field, and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Subject Alternative Name	Subject Alternative Names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. For example, SANs are used to protect multiple domain names such as www.example.com and www.example.net, in contrast to wildcard certificates that can only protect all first-level subdomains on one domain, such as *.example.com. This section is not available is the certificate type is *Intermediate CA certificate signing request (CSR)*.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the user principal name used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Additional Options	
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires. This option is not available is the certificate type is set to *Intermediate CA certificate signing request (CSR)*.
Key type	The key type is set to RSA.

Key size	Select the key size from the drop-down list: 1024, 2048, or 4096 bits.
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.

3. Select *OK* to create the new CA certificate.

Importing CA certificates and signing requests

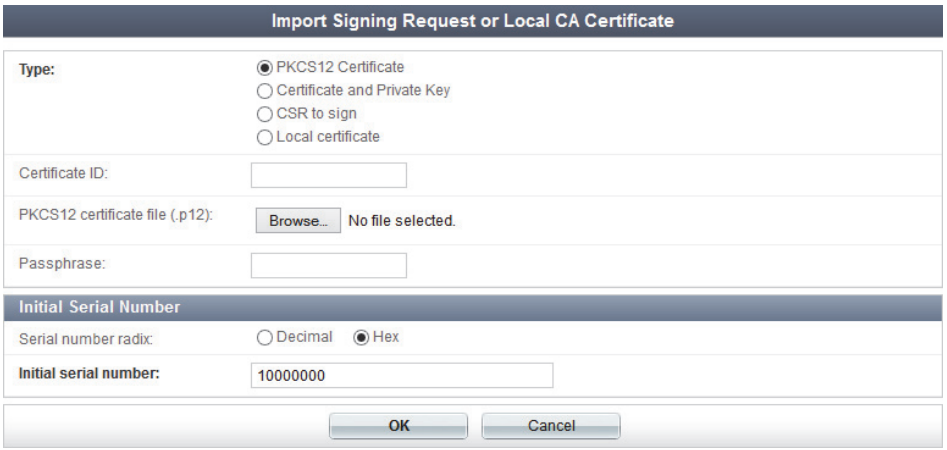
Four options are available when importing a certificate or signing request: *PKCS12 Certificate*, *Certificate and Private Key*, *CSR to sign*, and *Local certificate*.

To import a PKCS12 certificate:

1. From the local CA certificate list, select *Import*.

   The *Import Signing Request or Local CA Certificate* window opens.
2. Select *PKCS12 Certificate* in the type field.

Figure 117: Import a PKCS12 certificate



3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
PKCS12 certificate file (.p12)	Select *Browse...* to locate the certificate file on your computer.
Passphrase	Enter the certificate passphrase.
Initial serial number	Select the serial number radix, either decimal or hex, in the *Serial number radix* field, then enter the initial serial number in the *Initial serial number* field.

4. Select *OK* to import the certificate.

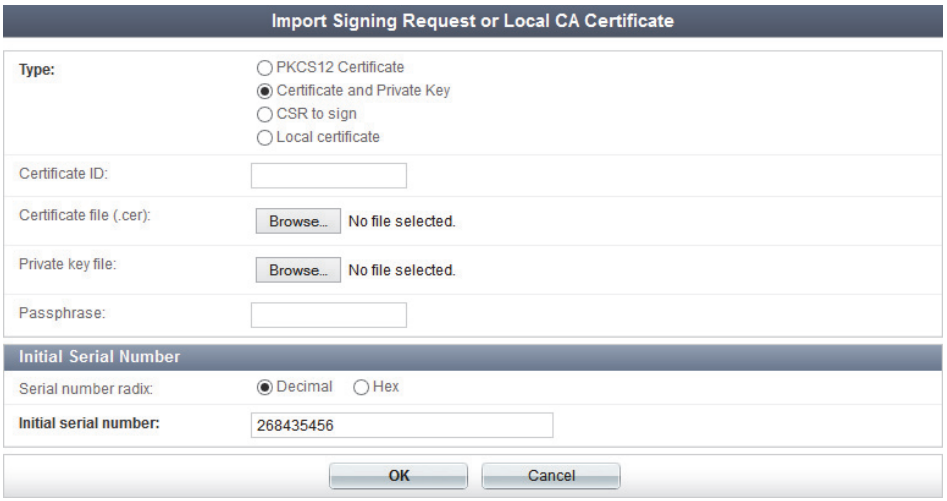
To import a certificate with a private key:

1. From the local CA certificate list, select *Import*.

   The *Import Signing Request or Local CA Certificate* window opens.

2. Select *Certificate and Private Key* in the type field.

Figure 118: Import a certificate and private key



3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
Certificate file (.cer)	Select *Browse...* to locate the certificate file on your computer.
Private key file	Select *Browse...* to locate the private key file on your computer.
Passphrase	Enter the certificate passphrase.
Initial serial number	Select the serial number radix, either decimal or hex, in the *Serial number radix* field, then enter the initial serial number in the *Initial serial number* field.

4. Select *OK* to import the certificate.

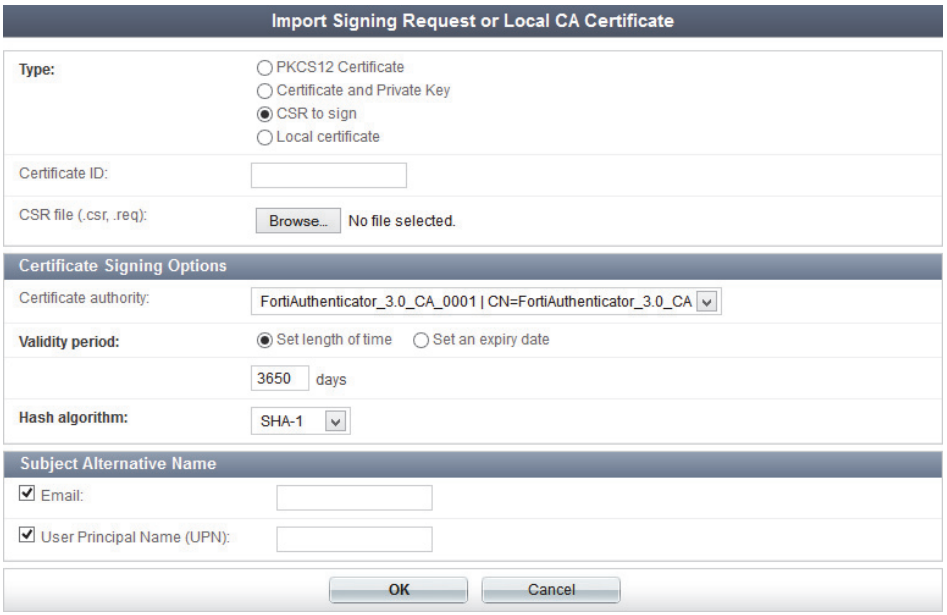
To import a CSR to sign:

1. From the local CA certificate list, select *Import*.

   The *Import Signing Request or Local CA Certificate* window opens.

2. Select *CSR to sign* in the type field.

Figure 119: Import a CSR to sign



3. Enter the following:

Certificate ID	Enter a unique ID for the certificate.
CSR file (.csr, .req)	Select *Browse...* to locate the CSR file on your computer.
Certificate Signing Options	
Certificate authority	Select one of the available CAs from the drop-down list.
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Subject Alternative Name	This section is not available is the certificate type is *Intermediate CA certificate signing request (CSR)*.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the user principal name used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.

4. Select *OK* to import the CSR.

To import a local CA certificate:

1. From the local CA certificate list, select *Import*.

   The *Import Signing Request or Local CA Certificate* window opens.
2. Select *Local certificate* in the type field.
3. Select *Browse...* in the *Certificate file (.cer)* field to locate the certificate file on your computer.
4. Select *OK* to import the local CA certificate.

CRLs

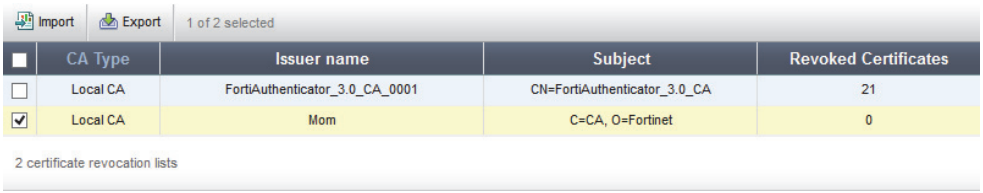
A CRL is a file that contains a list of revoked certificates, their serial numbers, and their revocation dates. The f ile also contains the name of the issuer of the CRL, the effective date, and the next update date. By default, the shortest validity period of a CRL is one hour.

Some potential reasons for certificates to be revoked include:

- A CA server was hacked and its certificates are no longer trustworthy,
- A single certificate was compromised and is no longer trustworthy,
- A certificates has expired and is not supposed to be used past its lifetime.

Go to *Certificate Management* > *Certificate Authorities* > *CRLs* to view the CRL list.

Figure 120:CRL list



The following information is shown:

Import	Import a CRL. See “To import a CRL:” on page 150.
Export	Save the selected CRL to your computer.
CA Type	The CA type of CRL.
Issuer name	The name of the issuer of the CRL.
Subject	The CRL’s subject.
Revoked Certifications	The number of revoked certificates in the CRL.

To import a CRL:

1. Download the most recent CRL from a CRL Distribution Point (CDP). One or more CDPs are usually listed in a certificate under the Details tab.
2. From the CRL list, select *Import*.
3. Select *Browse...* to locate the file on your computer, then select *OK* to import the list.

   When successful, the CRL will be displayed in the CRL list on the FortiAuthenticator device. You can select it to see the details (see “To view certificate details:” on page 143).

Locally created CRLs

When you import a CRL, it is from another authority. If you are creating your own CA certificates, then you can also create your own CRL to accompany them.

As a CA, you sign user certificates. If for any reason you need to revoke one of those certificates, it will go on a local CRL. When this happens you need to export the CRL to all your certificate users so they are aware of the revoked certificate.

To create a local CRL:

1. Create a local CA certificate. See "Local CAs" on page 143.
2. Create one or more user certificates. See "End entities" on page 136.
3. Go to *Certificate Management* > *End Entities* > *Users*, select one or more certificates, and then select *Revoke*. See "To revoke a certificate:" on page 142.

   The selected certificates will be removed from the user certificate list (see Figure 109 on page 137), and a CRL will be created with those certificates as entries in the list. If there is already a CRL for the CA that signed the user certificates, the certificates will be added to the current CRL.

   If, at a later date, one or more CAs are deleted, their corresponding CRLs will also be deleted, along with any user certificates that they signed.

Configuring online certificate status protocol

FortiAuthenticator also supports Online Certificate Status Protocol (OCSP), defined in RFC 2560. To use OCSP, configure the FortiGate unit to use TCP port 2560 on the FortiAuthenticator IP address.

For example, configuring OCSP in FortiGate CLI for a FortiAuthenticator with an IP address of 172.20.120.16, looks like this:

```
config vpn certificate ocsp-server
  edit fac_ocsp
    set cert "REMOTE_Cert_1"
    set url "http://172.20.120.16:2560"
  end
```

Trusted CAs

Trusted CA certificates can be used to validate certificates signed by an external CA.

To view the trusted CA certificate list, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*.

The certificate ID, subject, issuer, and status are shown. Certificates can be imported, exported, and searched.

To import a trusted CA certificate:

1. From the trusted CA certificate list, select *Import*.

   The *Import Signing Request or Trusted CA Certificate* window opens.
2. Enter a certificate ID in the *Certificate ID* field.
3. In the *Certificate* field, Select *Browse...* to locate the file on your computer, then select *OK* to import the list.

   When successful, the trusted CA certificate will be displayed in the list on the FortiAuthenticator device. You can select it to see the details (see "To view certificate details:" on page 143).

SCEP

The FortiAuthenticator device contains a SCEP server that can sign user CSRs (see “Enrollment method” on page 152), and distribute CRLs and CA certificates. To use SCEP, you must:

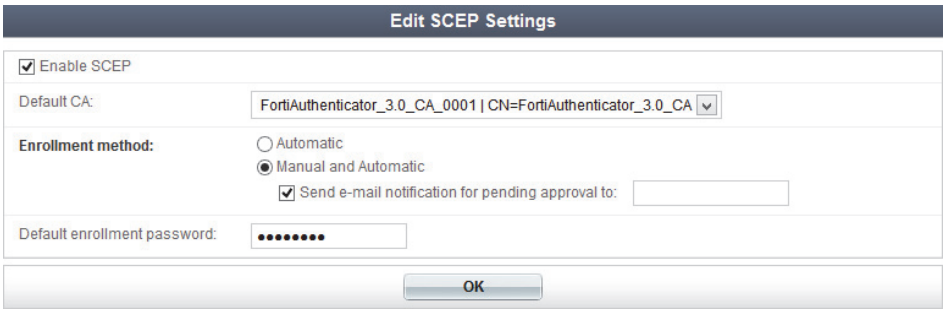
- Enable HTTP administrative access on the interface connected to the Internet. See “Interfaces” on page 42.
- Add the CA certificate for your certificate authority. See “Certificate authorities” on page 143.
- Select the CA to use for SCEP. See “Default CA” on page 152.

General

Users can request a user certificate through online SCEP. As administrator, you can allow the FortiAuthenticator unit to either automatically sign the user’s certificate or alert you about the request for signature.

To enable SCEP and configure general settings, go to *Certificate Management* > *SCEP* > *General*.

Figure 121: Edit SCEP settings



The following settings can be configured:

Enable SCEP	Select to enable SCEP.
Default CA	Select the default CA to use from the drop-down list.
Enrollment method	Select the enrollment method: • *Automatic*: The certificate is pre-approved by the administrator. The administrator enters the certificate information on the FortiAuthenticator unit and gives the user a challenger password to use when submitting their request. • *Manual and Automatic*: The user submits the CSR, the request shows up as pending on FortiAuthenticator unit, then the administrator manually approves the pending request. Optionally, enter an email address send pending approval notifications to.
Default enrollment password	Enter the default enrollment password that will be used when not setting a random password. See “To create a new certificate enrollment request:” on page 155.

Select *OK* to apply any changes you have made.

Enrollment requests

To view and manage certificate enrollment requests, go to *Certificate Management* > *SCEP* > *Enrollment Requests*.

Figure 122: Certificate enrollment requests

The following information is available:

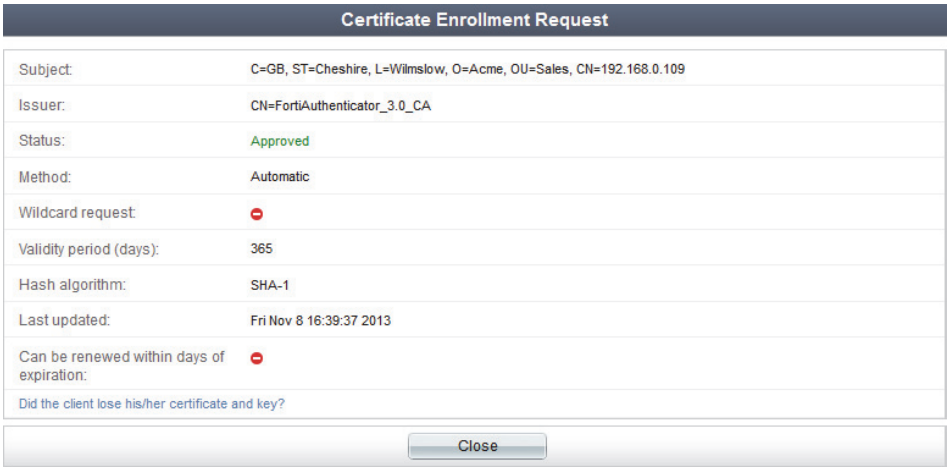
Create New	Create a new certificate enrollment request. See
Delete	Delete the selected certificate enrollment request.
Approve/Reject	Approve or reject the selected certificate enrollment request.
Method	The enrollment method used.
Status	The status of the enrollment: pending, approved, or rejected.
Wildcard	If it is a wildcard request, a green circle with a check mark is shown.
Issuer	The issuer of the certificate.
Subject	The certificate subject.
Renewable Before Expiry (days)	The number of days before the certificate enrollment request expires that it can be renewed.
Updated at	The date and time that the enrollment request was last updated.

To view the enrollment request details:

1. From the enrollment request list, select a request by clicking within its row.

   The *Certificate Enrollment Request* window opens.

Figure 123: Certificate enrollment request details



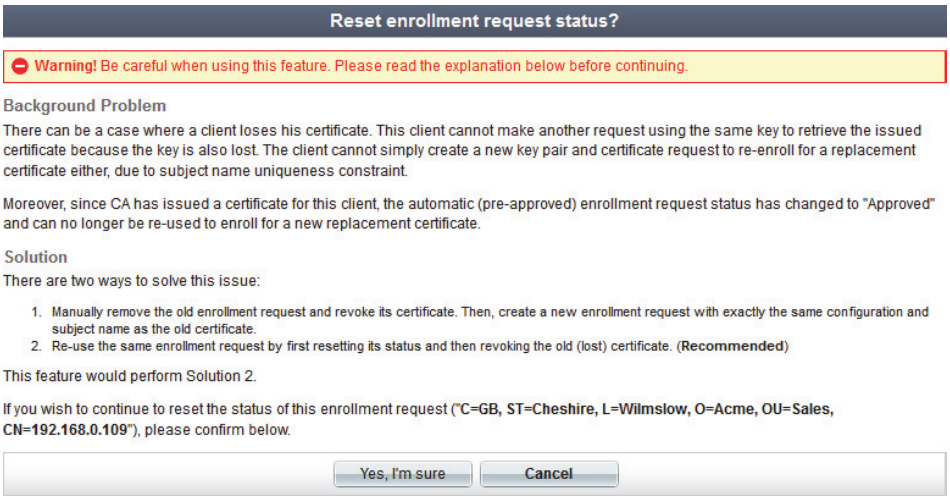
2. If the client has lost their certificate and key, select *Did the client lose his/her certificate and key?*
3. Select *Close* to return to the enrollment request window.

To reset the enrollment request status:

1. From the Certificate Enrollment Request window, select *Did the client lose his/her certificate and key?*

   The *Reset enrollment request status?* window opens.

Figure 124: Reset enrollment request status



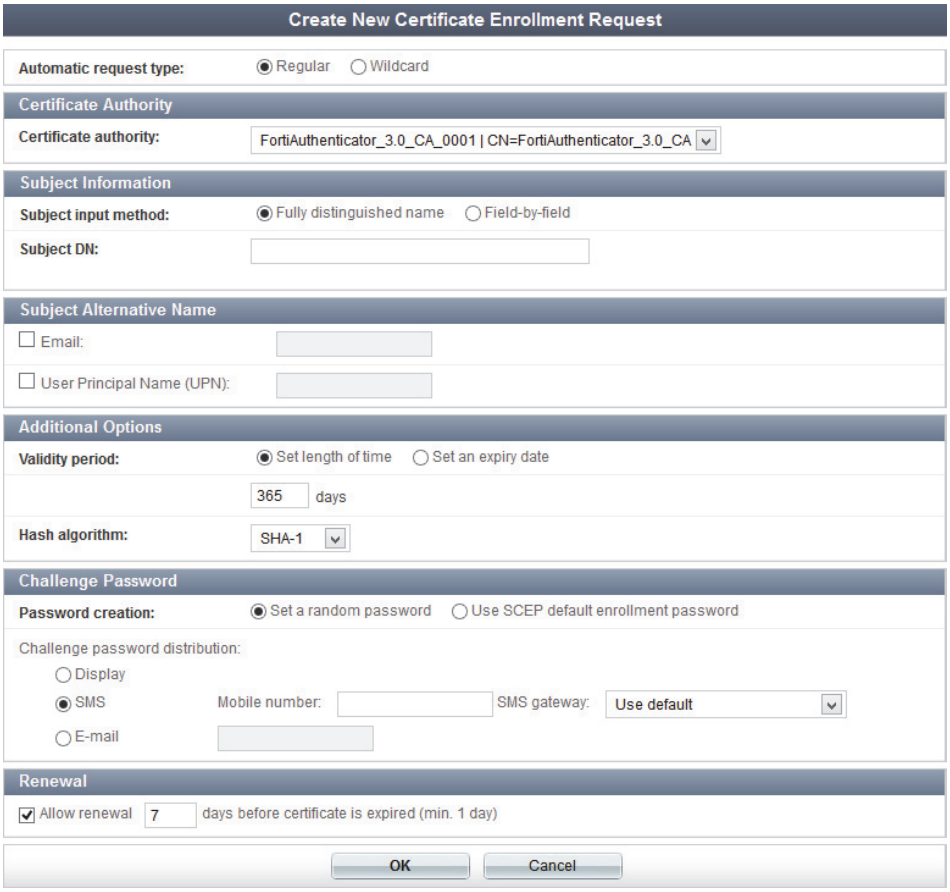
2. There are two methods to reset the enrollment request:
   - Manually remove the old enrollment request, revoke its certificate, then create a new enrollment request with exactly the same configuration and subject name as the old certificate.
   - Re-use the same enrollment request by resetting its status and then revoking the lost certificate.
3. To re-use the same enrollment request, select *Yes, I'm sure*. This is the recommended method of resolving the issue.

To create a new certificate enrollment request:

1. From the certificate enrollment requests list, select *Create New*.

   The *Create New Certificate Enrollment Request* window opens.

Figure 125: Create a new certificate enrollment request



2. Enter the following information:

Automatic request type	Select the automatic request type, either *Regular* or *Wildcard*.
Certificate Authority	Select one of the available CAs configured on the FortiAuthenticator unit from the drop-down list. The CA must be valid and current. If it is not you will have to create or import a CA certificate before continuing. See "Certificate authorities" on page 143.
Subject Information	
Subject input method	Select the subject input method, either *Fully distinguished name* or *Field-by-field*.
Subject DN	If the subject input method is *Fully distinguished name*, enter the full distinguished name of the subject. There should be no spaces between attributes. Valid DN attributes are DC, C, ST, L, O, OU, CN, and emailAddress. They are case-sensitive.

Field-by-field	If the subject input method is field-by-field, enter the subject name in the *Name (CN)* field (if the *Automatic request type* is set to *Regular*), and optionally enter the following fields: • *Department (OU)* • *Company (O)* • *City (L)* • *State/Province (ST)* • *Country (C)* (select from drop-down list) • *E-mail address*
Subject Alternative Name	This option is only available if the *Automatic request type* is set to *Regular*.
Email	Enter the email address of a user to map to this certificate.
User Principal Name (UPN)	Enter the user principal name used to find the user's account in Microsoft Active Directory. This will map the certificate to this specific user. The UPN is unique for the Windows Server domain. This is a form of one-to-one mapping.
Additional Options	
Validity period	Select the amount of time before this certificate expires. Select *Set length of time* to enter a specific number of days, or select *Set an expiry date* and enter the specific date on which the certificate expires.
Hash algorithm	Select the hash algorithm from the drop-down list, either SHA-1 or SHA-256.
Challenge Password	
Password creation	Select to either set a random password, or use the default enrollment password (see "Default enrollment password" on page 152).
Challenge password distribution	Select the challenge password distribution method. This option is only available if *Password creation* is set to *Set a random password*. • *Display*: display the password on the screen. • *SMS*: send the password to a mobile phone. Enter the phone number in the *Mobile number* field and select an SMS gateway from the drop-down list. • *E-mail*: send the password to the email address entered in the email field.
Renewal	To allow renewals, select *Allow renewal*, then enter the number of days before the certificate expires.

3. Select *OK* to create the new certificate enrollment request.

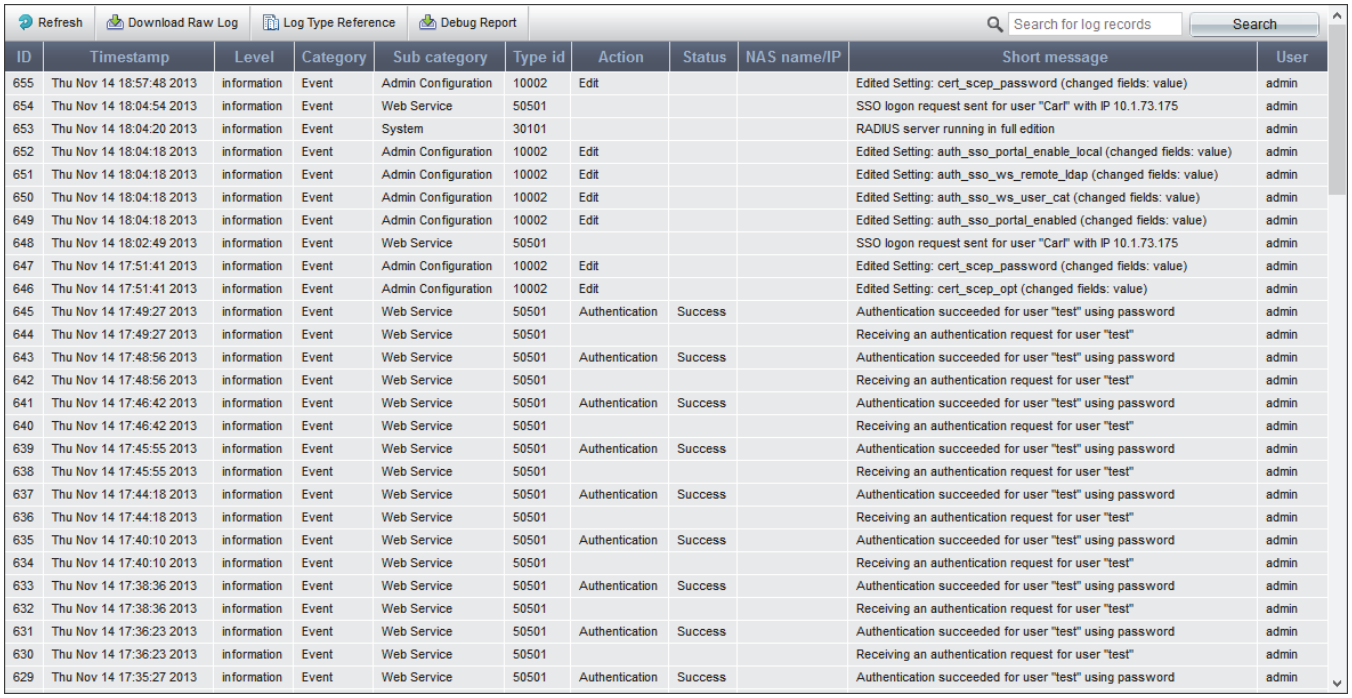
Logging

Accounting is an important part of FortiAuthenticator. The *Logging* menu tree provides a record of the events that have taken place on the FortiAuthenticator unit.

Log access

To view the log events table, go to *Logging* > *Log Access* > *Logs*.

Figure 126: Logs



ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	NAS name/IP	Short message	User
655	Thu Nov 14 18:57:48 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: cert_scep_password (changed fields: value)	admin
654	Thu Nov 14 18:04:54 2013	information	Event	Web Service	50501				SSO logon request sent for user "Carl" with IP 10.1.73.175	admin
653	Thu Nov 14 18:04:20 2013	information	Event	System	30101				RADIUS server running in full edition	admin
652	Thu Nov 14 18:04:18 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: auth_sso_portal_enable_local (changed fields: value)	admin
651	Thu Nov 14 18:04:18 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: auth_sso_ws_remote_ldap (changed fields: value)	admin
650	Thu Nov 14 18:04:18 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: auth_sso_ws_user_cat (changed fields: value)	admin
649	Thu Nov 14 18:04:18 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: auth_sso_portal_enabled (changed fields: value)	admin
648	Thu Nov 14 18:02:49 2013	information	Event	Web Service	50501				SSO logon request sent for user "Carl" with IP 10.1.73.175	admin
647	Thu Nov 14 17:51:41 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: cert_scep_password (changed fields: value)	admin
646	Thu Nov 14 17:51:41 2013	information	Event	Admin Configuration	10002	Edit			Edited Setting: cert_scep_opt (changed fields: value)	admin
645	Thu Nov 14 17:49:27 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
644	Thu Nov 14 17:49:27 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
643	Thu Nov 14 17:48:56 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
642	Thu Nov 14 17:48:56 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
641	Thu Nov 14 17:46:42 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
640	Thu Nov 14 17:46:42 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
639	Thu Nov 14 17:45:55 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
638	Thu Nov 14 17:45:55 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
637	Thu Nov 14 17:44:18 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
636	Thu Nov 14 17:44:18 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
635	Thu Nov 14 17:40:10 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
634	Thu Nov 14 17:40:10 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
633	Thu Nov 14 17:38:36 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
632	Thu Nov 14 17:38:36 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
631	Thu Nov 14 17:36:23 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin
630	Thu Nov 14 17:36:23 2013	information	Event	Web Service	50501				Receiving an authentication request for user "test"	admin
629	Thu Nov 14 17:35:27 2013	information	Event	Web Service	50501	Authentication	Success		Authentication succeeded for user "test" using password	admin

The following options and information are available:

Refresh	Refresh the log list.
Download Raw Log	Export the FortiAuthenticator log to your computer as a text file named *fac.log*.
Log Type Reference	Select to view the log type reference dialog box. See “Log type reference” on page 159.
Debug Report	Select to download the debug report to your computer as a file named *report.dbg*.

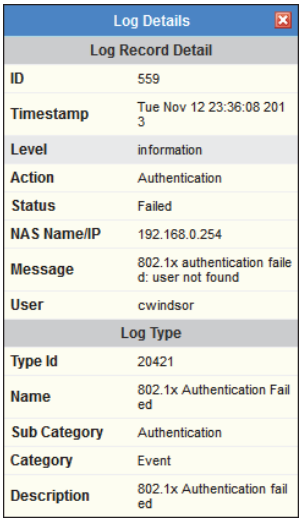
Search	Enter a search term in the search field, then select *Search* to search the log message list. The search string must appear in the Message portion of the log entry to result in a match. To prevent each term in a phrase from being matched separately, multiple keywords must be in quotes and be an exact match. After the search is complete the number of positive matches will be displayed next to the Search button, with the total number of log entries in brackets following. Select the total number of log entries to return to the full list. Subsequent searches will search all the log entries, and not just the previous search's results.
ID	The log message's ID.
Timestamp	The time the message was received.
Level	The log severity level: • *Emergency*: The system has become unstable. • *Alert*: Immediate action is required. • *Critical*: Functionality is affected. • *Error*: An erroneous condition exists, and functionality is probably affected. • *Warning*: Functionality could be affected. • *Notification*: Information about normal events. • *Information*: General information about system operations. • *Debug*: Detailed information useful for debugging purposes.
Category	The log category, which is always *Event*. See "Log type reference" on page 159.
Sub category	The log subcategory. See "Log type reference" on page 159.
Type id	The log type ID.
Action	The action which created the log message.
Status	The status if the action that created the log message, if applicable.
NAS name/IP	The NAS name or IP address of the relevant device if an authentication action fails.
Short message	The log message itself, shortened.
User	The user to whom the log message pertains.

To view log details:

1. From the log list, select the log whose details you need to view by clicking anywhere within the log's row.

   The *Log Details* pane will open on the right side of the window.

   Figure 127: Log details

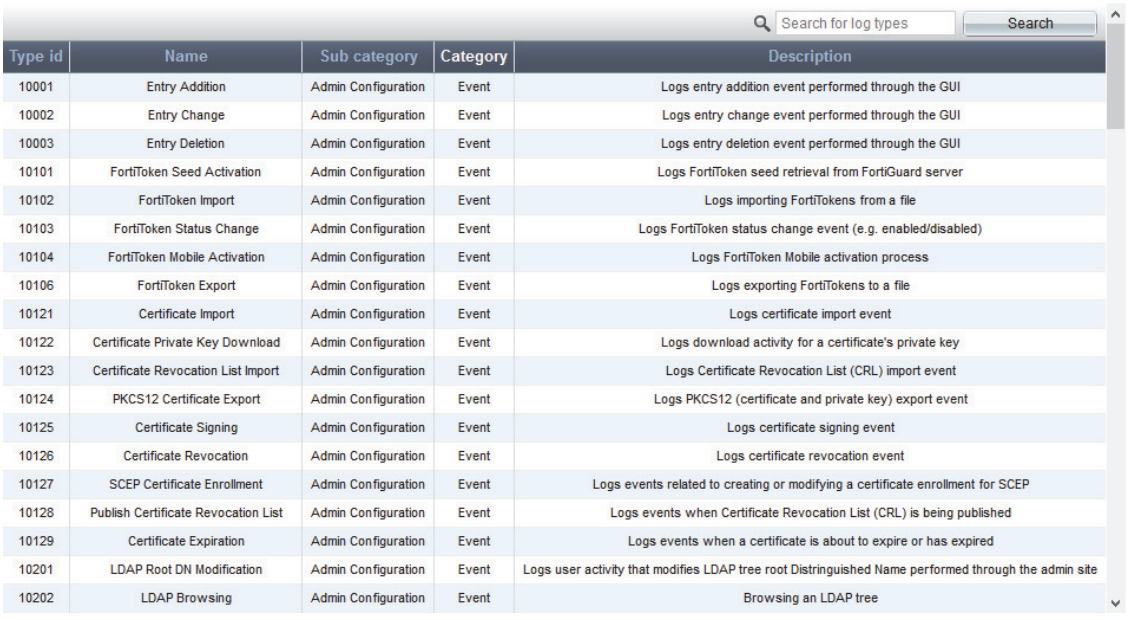


2. After viewing the log details, select the close icon in the top right corner of the pane to close the details pane.

Log type reference

Select *Log Type Reference* in the log list toolbar to open the log type reference dialog box.

Figure 128: Log type reference



Type id	Name	Sub category	Category	Description
10001	Entry Addition	Admin Configuration	Event	Logs entry addition event performed through the GUI
10002	Entry Change	Admin Configuration	Event	Logs entry change event performed through the GUI
10003	Entry Deletion	Admin Configuration	Event	Logs entry deletion event performed through the GUI
10101	FortiToken Seed Activation	Admin Configuration	Event	Logs FortiToken seed retrieval from FortiGuard server
10102	FortiToken Import	Admin Configuration	Event	Logs importing FortiTokens from a file
10103	FortiToken Status Change	Admin Configuration	Event	Logs FortiToken status change event (e.g. enabled/disabled)
10104	FortiToken Mobile Activation	Admin Configuration	Event	Logs FortiToken Mobile activation process
10106	FortiToken Export	Admin Configuration	Event	Logs exporting FortiTokens to a file
10121	Certificate Import	Admin Configuration	Event	Logs certificate import event
10122	Certificate Private Key Download	Admin Configuration	Event	Logs download activity for a certificate's private key
10123	Certificate Revocation List Import	Admin Configuration	Event	Logs Certificate Revocation List (CRL) import event
10124	PKCS12 Certificate Export	Admin Configuration	Event	Logs PKCS12 (certificate and private key) export event
10125	Certificate Signing	Admin Configuration	Event	Logs certificate signing event
10126	Certificate Revocation	Admin Configuration	Event	Logs certificate revocation event
10127	SCEP Certificate Enrollment	Admin Configuration	Event	Logs events related to creating or modifying a certificate enrollment for SCEP
10128	Publish Certificate Revocation List	Admin Configuration	Event	Logs events when Certificate Revocation List (CRL) is being published
10129	Certificate Expiration	Admin Configuration	Event	Logs events when a certificate is about to expire or has expired
10201	LDAP Root DN Modification	Admin Configuration	Event	Logs user activity that modifies LDAP tree root Distringuished Name performed through the admin site
10202	LDAP Browsing	Admin Configuration	Event	Browsing an LDAP tree

The following information is available:

Search	Enter a search term in the search field, then select *Search* to search the log type reference.
Type id	The log type ID.
Name	The name of the log type.
Sub category	The log type subcategory, one of: *Admin Configuration*, *Authentication*, *System*, or *User Portal*.
Category	The log type category, which is always *Event*.
Description	A brief description of the log type.

To close the *Log Type Reference* dialog box, select *close* above the top right corner of the box, or simply click anywhere outside of the box within the log list.

Sort the log messages

The log message table can be sorted by any column. To sort the log entries by a particular column, select the title for that column. The log entries will now be displayed based on data in that column in ascending order. Ascending or descending is displayed with an arrow next to the column title, an up arrow for ascending and down arrow for descending.

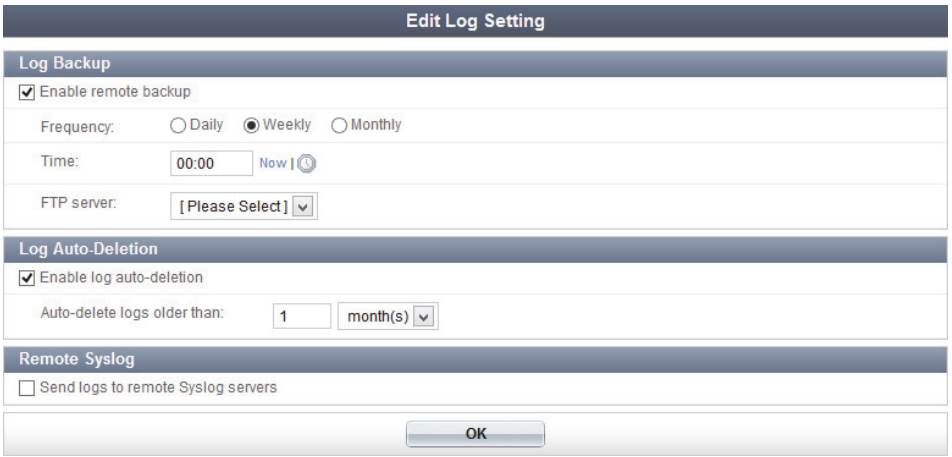
Log configuration

Logs can be remotely backed up to an FTP server, automatically deleted, and sent to a remote syslog server in lieu of storing them locally.

Log settings

To configure log backups, automatic deletion, and remote storage, go to *Logging* > *Log configuration* > *Log Setting*.

Figure 129: Log settings



To configure log backups:

1. In the log settings window, select *Enable remote backup* in the *Log Backup* section.
2. Select the frequency of the backups in the *Frequency* field, one of *Daily*, *Weekly*, or *Monthly*.
3. Configure the time of day that the backup will occur in one of the following ways:
   - Enter a time in the *Time* field
   - Select *Now* to enter the current time
   - Select the clock icon and choose a time from the pop-up menu: *Now*, *Midnight*, *6 a.m.*, or *Noon*.
4. Select an FTP server from the drop-down list in the *FTP server* field. For information on configuring an FTP server, see "FTP Servers" on page 56.
5. Select *OK* to save your settings.

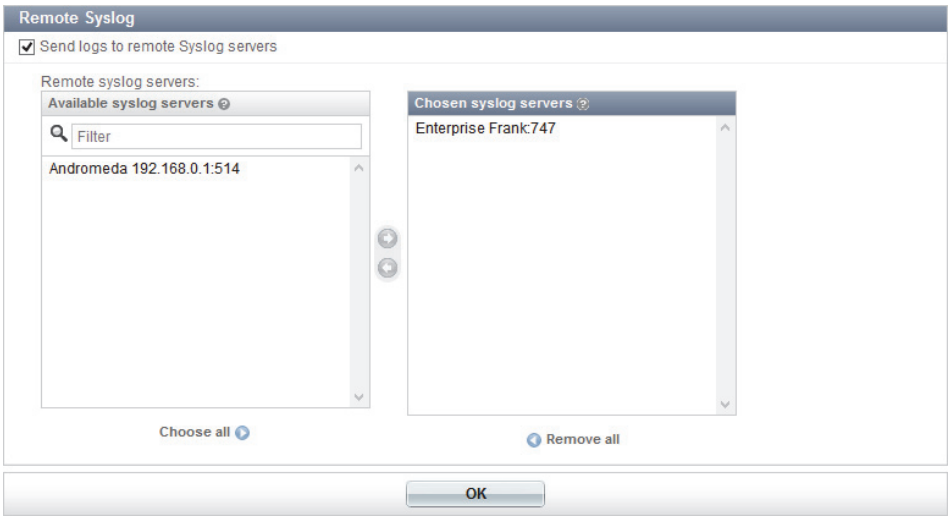
To configure automatic log deletion:

1. In the log settings window, select *Enable log auto-deletion* in the *Log Auto-Deletion* section.
2. In the *Auto-delete logs older* than field, select *day(s)*, *week(s)*, or *month(s)* from the drop-down list, then enter the number of days, weeks, or months, after which a log will be deleted.
3. Select *OK* to save your settings.

To configure logging to a remote syslog server:

1. In the log settings window, select *Send logs to remote Syslog servers* in the *Remote Syslog* section.

   Figure 130: Send logs to remote syslog servers



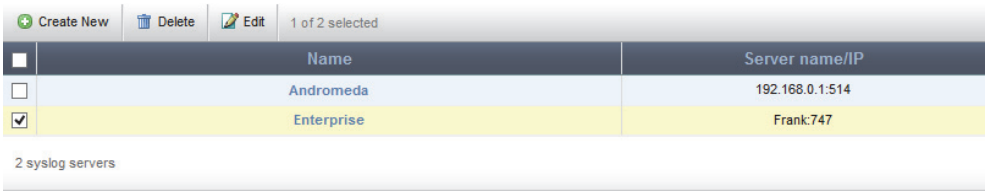
2. Move the syslog servers to which the logs will be sent from the *Available syslog servers* box to the *Chosen syslog servers* box.

   For information on adding syslog servers, see "Syslog servers" on page 162.
3. Select *OK* to save your settings.

Syslog servers

Syslog servers can be used to store remote logs, see "To configure logging to a remote syslog server:" on page 161. To view the syslog server list, go to *Logging* > *Log Config* > *Syslog Servers*.

Figure 131: Syslog servers

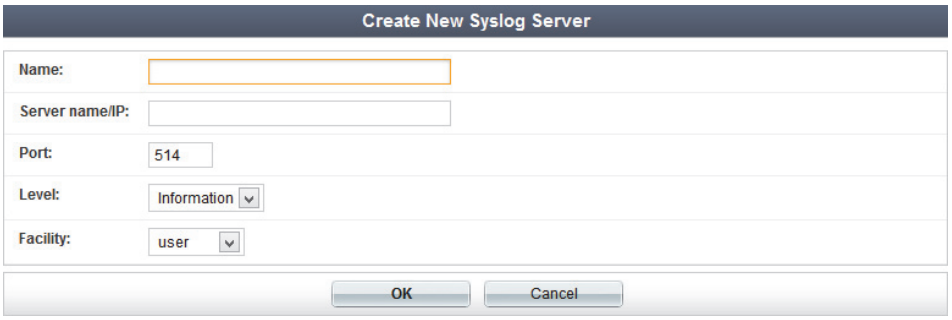


Create New	Add a new syslog server. See "To add a syslog server:" on page 162.
Delete	Delete the selected syslog server or servers.
Edit	Edit the selected syslog server.
Name	The syslog server name on the FortiAuthenticator unit.
Server name/IP	The server name or IP address, and port number.

To add a syslog server:

1. From the syslog servers list, select *Create New*.
   The *Create New Syslog Server* window opens.

   Figure 132: Create a new syslog server



2. Enter the following information:

Name	Enter a name for the syslog server on the FortiAuthenticator unit.
Server name/IP	Enter the syslog server name or IP address.
Port	Enter the syslog server port number. The default port is 514.
Level	Select a log level to store on the remote server from the drop down list. See "Level" on page 158.
Facility	Select a facility from the drop-down list.

3. Select *OK* to add the syslog server.

Troubleshooting

This chapter provides suggestions to resolve common problems encountered while configuring and using your FortiAuthenticator device, as well as information on viewing debug logs.

For more support, contact Fortinet Customer Service & Support (support.fortinet.com).

Before starting, please ensure that your FortiAuthenticator device is plugged in to an appropriate, and functional, power source.

Troubleshooting

The following table describes some of the basic issues that can occur while using your FortiAuthenticator device, and suggestions on how to solve said issues.

Table 8: Troubleshooting

Problem	Suggestions
All user login attempts fail, there is no response from the FortiAuthenticator device, and there are no entries in the system log.	• Check that the authentication client has been correctly configured. See "Adding a FortiAuthenticator unit to your network" on page 24. If the authentication client is not configured, all requests are silently dropped. • Verify that traffic is reaching the FortiAuthenticator device. Is there an intervening Firewall blocking 1812/UDP RADIUS Authentication traffic, is the routing correct, is the authentication client configured with correct IP address for the FortiAuthenticator unit, etc.
All user login attempts fail with the message *RADIUS ACCESS-REJECT*, and *invalid password* in shown in the logs.	• Verify that the authentication client secrets are identical to those on the FortiAuthenticator unit.

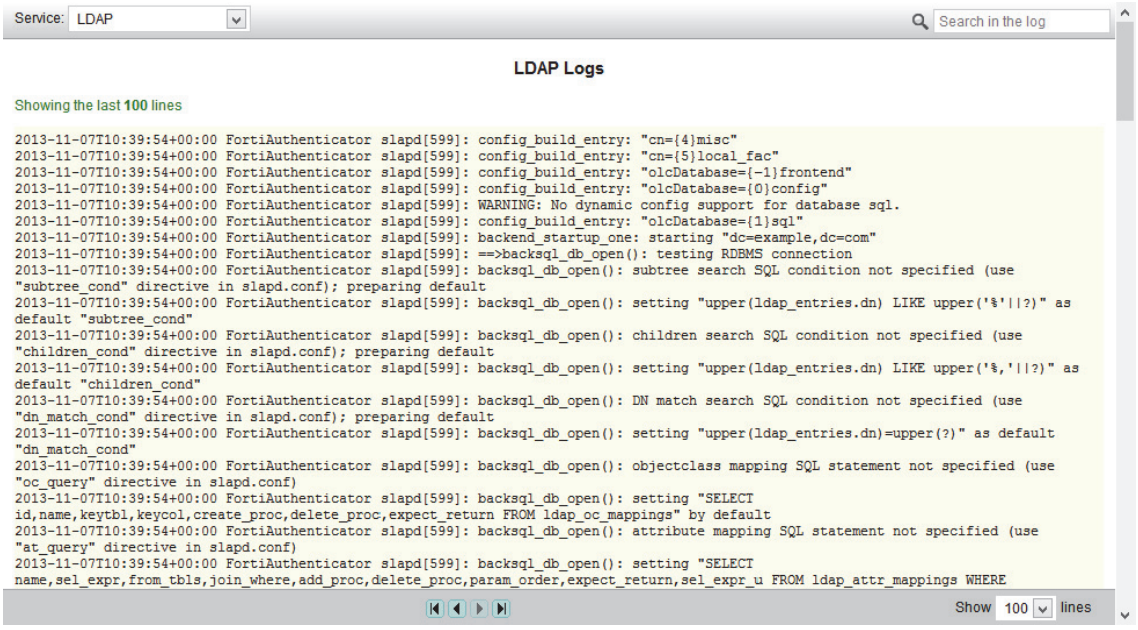
Table 8: Troubleshooting

Problem	Suggestions
Generally, user login attempts are successful, however, an individual user authentication attempt fails with *invalid password* in shown in the logs.	• Reset the user's password and try again. See "Editing a user" on page 73. • Have the user privately show their password to the administrator to check for unexpected characters (possibly due to keyboard regionalization issues).
Generally, user login attempts are successful, however, an individual user authentication attempt fails with *invalid token* in shown in the logs.	• Verify that the user is not trying to use a previously used PIN. Tokens are One Time Passwords, so you cannot log in twice with the same PIN. • Verify that the time and timezone on the FortiAuthenticator unit are correct and, preferably, synchronised using NTP. See "Configuring the system time, time zone, and date" on page 36. • Verify that the token is correctly synchronized with the FortiAuthenticator unit, and verify the drift by synchronizing the token. See "FortiToken drift adjustment" on page 89. • Verify the user is using the token assigned to them (validate the serial number against the FortiAuthenticator unit configuration). See "User management" on page 70. • If the user is using an e-mail or SMS token, verify it is being used within the valid timeout period. See "Lockouts" on page 67.

Debug logs

Extended debug logs can be accessed by using your web browser to browse to `https://<FortiAuthenticator IP Address>/debug`.

Figure 133: Debug logs



Service	Select the service whose logs are shown from the drop-down list. The options are: • FSSO Agent • GUI • HA • LDAP • RADIUS Accounting • RADIUS Authentication • SNMP • Startup • Web Server
Search	Enter a search term in the search field, then select *Search* to search the debug logs.
Page navigation	Use the *First Page*, *Previous Page*, *Next Page*, and *Last Page* icons to navigated through the logs.
Show	Select the number of lines to show per page from the drop-down list. The options are: *100* (default), *250*, and *500*.

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W